



ACCEPTABLE USE POLICY FOR PUPILS

INTRODUCTION

This is an important document which covers our policies for and the use of:

- ICT and electronic equipment;
- Cloud based platforms;
- Digital and video images of pupils;
- Biometric data.

The information below explains expectations for pupils using our ICT systems, what electronic systems and facilities we make use of in school and how we may wish to use and store the personal data of pupils.

This document should be read in conjunction with the John Taylor Multi-Academy Trust (JTMAT) Data Protection Policy and Records Management (GDPR) Policy which fully explains how your data will be used and processed. These can be found by visiting <https://jtmat.co.uk/privacy/policies/>

Please read this information carefully and then indicate your acceptance of these policies (if any) at the end of this document and return the form to school. Your response to this document will be stored digitally in school for our records.

ICT AND ELECTRONIC EQUIPMENT ACCEPTABLE USE POLICY - OVERVIEW

This is a statement of good computer practices to protect Chase Terrace Academy, its pupils, staff and all equipment from casual or intentional abuse. With the prolific use of e-mail, mobile technology and access to the Internet throughout the school there are a number of threats and legal risks to the school, as well as the potential costs of time wasting that can be avoided by following the practices outlined. Although these tools are provided first and foremost for school use, Chase Terrace Academy accepts that on occasion they may be used for personal use, however this should be kept to a minimum. Users should take in to account these guidelines and adhere to them at all times.

These guidelines apply to all pupils who have access to email, the internet, any computer systems, mobile phones or any other relevant electronic device being used whilst on school premises, school owned equipment or any device connected to the school network at any time and in any place.

All users will be notified of these Acceptable Use Policies, via a logon screen which will appear whenever a user logs on. To proceed, users will have to click on a button that states, "By logging on to the school system, I accept all Chase Terrace Academy policies on the use of IT systems and equipment including email and the internet." New pupils will not be given access to e-mail, the Internet or any Chase Terrace Academy IT systems until they have seen and accepted these policies.

PRIVACY AND SAFEGUARDING

All users should be aware that Chase Terrace Academy takes the security and safety of all users very seriously. As a result, the school makes use of Proxy, Firewall, Filtering and Monitoring software to monitor all internet and PC usage. These systems are checked and monitored by ICT support staff on a regular basis, and some systems may also produce reports of concerns and infringements automatically. Although Chase Terrace Academy respects privacy, in the context of safeguarding and the safe provision and monitoring of ICT services, users should not have any expectation of privacy whilst using school systems and should not conduct any personal or sensitive business on school systems, including the sending and receiving of personal email. You should be aware that all text entry, regardless of the application being used is monitored for key words that may be deemed unsafe, inappropriate, or defamatory.

USE OF ICT EQUIPMENT

Pupils are granted access to a wide range of technology and equipment within school. This may include desktop PCs, laptops, tablet computers, biometric systems, design and technology (cad/cam) machines, sound/lighting equipment. Pupils must treat all equipment with respect, adhering to any health and safety procedures, display safe working practises and report immediately any faults or damage to ICT services or their teacher. Any wilful damage to school equipment will be pursued by the school.

Pupils will be provided a unique username and will be expected to set a password which conforms to the complexity requirements set. This is usually a password which is more than 8 characters in length and contains a mixture of upper and lower-case characters, plus numeral/s or symbol/s. Pupils are **solely** responsible for keeping their username and password safe and must never reveal their password to any other pupil, write it down or leave it anywhere where it could be abused by another individual.

Pupils are solely responsible for any legal, moral and professional issues that may arise through their actions using any electronic equipment or systems. Pupils should therefore ensure their familiarity with all related policies, if in doubt please seek advice from ICT support, Tutors, or your Heads of Year. Pupils should be aware that any inappropriate use of any electronic systems may lead to disciplinary action being taken, in extreme cases possibly exclusion or permanent exclusion. Pupils are responsible for maintaining the security of their account and must never share their password with any other individual as any misuse of ICT can be linked directly to the pupils' assigned user account.

Pupils are not permitted under any circumstances to use any school ICT equipment for the purpose of:

- File sharing
- Gambling
- Gaming
- Online purchases
- Installing software

- Circumventing or tampering with settings and security measures
- Any form of activity that could be considered dangerous or illegal

Failure to adhere to the terms of the acceptable use policy will result in disciplinary action as set out in the school behaviour policy against any users who are found to breach the policies outlined in these guidelines. The school reserves the right to suspend system access for an individual user without notice or reason.

USE OF THE INTERNET, EMAIL AND COMMUNICATION TOOLS

Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations. The wilful or deliberate display of emails or documents attached to emails containing any of the following will be considered a serious matter that will be dealt with in accordance with the school behaviour policy:

- Obscenities;
- Offensive language;
- Any mention of, or reference to, illegal activity;
- Discriminatory/extremist language, references or inferences;
- Sexually explicit content;
- Any other content which may be deemed unreasonable or unacceptable in a school context.

Pupils should never let anyone else use their school email account and should make every effort to apply a common-sense approach to using their email accounts:

- Do not open emails from recipients you do not recognise;
- Never open email attachments unless you are sure of the source;
- Use your school email account in any communication with organisations or individuals outside of school for school purposes (for example when organising a work experience placement);
- Use basic email etiquette – no capitals, always include a subject and always use an appropriate greeting;

Pupils have access to the internet and this is both filtered and monitored for the safety of our pupils and staff. Filtering software and rules, however, are not fool proof and it is simply not possible to block/filter all websites which may be inappropriate or cause distress to individuals. Whilst we take all possible precautions to protect our staff and pupils, Chase Terrace Academy cannot under any circumstances guarantee the safety of pupils using our internet provision.

Under no circumstances should a user access a site that contains sexually explicit, offensive, racist, extremist or illegal material. Should a pupil access a website that is inappropriate or they feel is unsuitable, they should immediately close their web browser and inform a teacher or ICT services who will then take steps to block the site in school.

We have an active programme of e-safety education and as such pupils should be well equipped to spot, avoid and report any online behaviour that is in any way inappropriate. If in school, pupils should report any concerns immediately to any member of staff who will then ensure the situation is addressed. If outside of school or

a pupil feels they cannot discuss a matter with a member of staff, then they should use the National Crime Agency online reporting tools which can be found on <https://ceop.police.uk/safety-centre/>

Misuse of the internet in school may result in the suspension of any user accounts involved pending further investigation or action.

PRINTING

We provide both colour and black and white printing in school. Pupils are not charged for printing at Chase Terrace Academy. We do, however, operate a system whereby we can set limits on the amount of pages each user may print. Furthermore, we actively monitor the use of our printing systems and reserve the right to immediately remove the ability to print from any user found to be abusing or circumventing our quota system.

Pupils should consider the need for printing and, wherever possible, should always consider using suitable electronic alternatives such as PDF documents which can be viewed on any computer, laptop, phone or tablet. As a general guideline, any document which is not class work or coursework should **not** be printed in school. Pupils that need exam or specification material should arrange this with their class teacher who may print these through our reprographics department.

USE OF PERSONAL MOBILE TECHNOLOGY (BYOD) AND SOCIAL MEDIA

It is imperative that both parents/carers and pupils understand that no school has the facilities to monitor and protect pupils whilst they are using mobile data services (3G, 4G or similar). It is for this reason that we cannot take any responsibility for pupil actions whilst using devices that are making use of mobile data. However, as with all other use of ICT in school our same expectations and rules apply and any misuse of mobile equipment in school regardless of the communication method used, still falls under the school's acceptable use policy and therefore the school behaviour policy also.

At Chase Terrace Academy, we recognise the importance of mobile devices to both parents/carers and pupils. As a school, however, we do not allow their use during lessons under any circumstances for any purpose unless under direct instruction from the classroom teacher. Pupils must never use their mobile devices to take pictures or videos of any member of staff or another pupil. Failure to adhere to this policy can result in serious disciplinary action being taken.

KS3 and KS4 pupils are not allowed to connect, or attempt to connect, their device to any of the school wireless networks without the explicit permission of ICT services. Any pupil who wishes to use their device on our network must contact ICT Services.

Chase Terrace Academy will provide basic internet filtering to internet access provided for mobile devices. We will not take any responsibility for misuse, data loss or any kind of virus/malware that may become installed on a device whilst in school. It is the responsibility of pupils to make sure that any device they use is suitably up to date and protected. We do not provide any kind of insurance or coverage for physical damage to pupil devices whilst they are on the premises.

We actively discourage the use of **any** social media whilst pupils are in school. Misuse of social media platforms can cause catastrophic consequences and are very difficult for the school to manage effectively. Chase Terrace Academy has absolutely no control over images, video or text posted to any social media platform on pupil's individual accounts, and we cannot guarantee that any requests to social media organisations to remove content will be actioned. Any pupil that is found to be posting any material that on social media that falls into the following categories will be dealt with to the full extent of the school behaviour policy:

- Images or video of any other pupil or member of staff without their explicit permission;
- Any text which could be:
 - offensive to another individual regardless of context;
 - Discriminatory (including, but not limited to racism, xenophobia, homophobia);
 - Extremist;
 - Obscene;
 - Illegal;
 - Defamatory;
 - Slanderous;

We actively carry out a program of education about the dangers of misusing social media and would take this opportunity to remind pupils that they should **never under any circumstances** meet or arrange to meet an individual they have met online. Any such approaches should be immediately reported to a member of staff.

COPYRIGHT

Pupils are reminded that material found online should be presumed to be the intellectual property of the author and, as such, should either seek to find if material is free for educational use or whether permission can be granted for content to be used in their work. There is obviously a case for "fair use" of material found online, but if in doubt pupils should seek help from a member of staff or the ICT support team. Any material that a pupil uses from the internet should be clearly referenced in their work.

CLOUD BASED PLATFORMS

A cloud-based system is simply any service which is provided by an external organisation and is accessed through the internet. In the context of our school we use a number of industry standard online systems to support pupils in school.

Pupils are given access to a range of online facilities which provide a range of learning opportunities and tools to assist in their work.

The school's primary online system is Microsoft Office 365, wherever possible, this is used as a centralised method of access to other online services.

Office 365 will provide your child with the ability to access work at home, to produce work using online tools through a web browser and have access to communication and organisational tools. Office 365 works on PC, mobile, mac and tablet computers. Some of the benefits are outlined below:

- **Mail** - an individual email account for school use managed by the school;
- **Calendar** - an individual calendar providing the ability to organize schedules, daily activities, and assignments;
- **Office Online** – pupils can access Word, Excel, OneNote, Powerpoint and more through a web browser – no install required;
- **OneDrive** – all pupils have access to 100gb of online cloud storage to enable them to store, backup and access work from home.
- **Office 365 Apps for home use** – The Microsoft Office suite of applications can be downloaded for educational use on personal devices

The school believes that use of the tools significantly adds to your child's educational experience.

The school's use of cloud services extends to its main information management system, safeguarding systems, backup, and biometric till systems.

Online platforms are often added, or removed from use as requirements change. An exhaustive list of online platforms in use is available on request.

By agreeing to this policy, you are confirming that:

- The school may create user accounts for your child on relevant services to support your child;
- You understand that, due to the nature of these being online services, a certain amount of personal data (names, user names, passwords) will inevitably stored on external servers out of the control of the school;
- The school expects pupils to follow safe and responsible working practises when using online facilities;
- You understand that your child will have access to these facilities outside of school and may be set tasks to complete using them. Furthermore, you understand that the school cannot monitor the use of online platforms outside of the school premises.

DIGITAL AND VIDEO IMAGES OF PUPILS

At Chase Terrace Academy, it is often the case that the use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used, for example, to review performances, in presentations or to perform evaluations.

Furthermore, images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Please note that for users of school transport, we would ideally need permission to use an image of the pupil for the purpose of their transport identification card.

The school makes every effort to comply with the Data Protection Act and we will, where appropriate or necessary, request parents / carers permission before taking

images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, it is essential that these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

By agreeing to this policy, you are confirming that:

- The school may take, store and use images of your child
- These images may be used primarily for learning and identification purposes
- Images may be used in school publications such as newsletters, the school website and prospectus.
- School may use images of pupils to promote individual pupil successes or achievements
- The school will take all reasonable precautions to protect the privacy of pupils.

BIOMETRIC DATA

The school uses biometric systems (fingerprint recognition) for the authentication of individual children for our catering facilities.

The use of biometric technologies in schools is now standard practise and in our school it drastically increases the efficiency of making payment in the school canteen. Furthermore, this system increases the safety of our pupils as they are not required to carry money or any form of identification (e.g. swipe card) in school. It is not possible for an individual to use any account other than their own.

The school has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified. No complete images of fingerprints are stored and it is not possible to reconstruct an image of a fingerprint from the data that is stored in our system.

Fingerprint data is held securely by our cloud cashless catering provider.

By agreeing to this policy, you are confirming that:

- The school may use electronic systems to store your child's fingerprint
- This data can then be used to uniquely identify your child

Version Tracking:

Date	Modified by	Notes
21-05-2025	O. Cooper	Updated wording on cloud providers, biometric and general changes