Acorn Trust
Staff Acceptable Usage Policy

Written by:	A Burkes
Date agreed:	Sept 2016
Next Review Date:	Autumn 2018
Chairs Signature	

Mission Statement

The Acorn Trust is a Multi-Academy Trust established with the aim of providing outstanding learning and opportunities for the children within its care.

Children are our nation's most precious resource. Their school life and learning experience will shape them for the whole of their lives

Safeguarding Statement

At the Acorn Trust we recognise our moral and statutory responsibility to safeguard and promote the welfare of all children.

We work to provide a safe and welcoming environment where children are respected and valued. We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice.

The procedures contained in the Safeguarding Policy apply to all staff, volunteers and governors

Acceptable Usage Policy

Contents

1 Introduction

The Trust encourages the use of its IT Systems and Services for communicating with pupils, parents and the wider community for business related purposes.

The aim of this guidance is to clearly outline what the Acorn Trust consider to be acceptable, unacceptable and forbidden use of their IT.

For the purposes of this guidance IT refers to system and applications, internet, e mail, telephone landlines, personal computers, laptops, ipads and servers. This is not an exhaustive list and will also cover future technology.

The guidance's aim is not to impose unnecessary restrictions, but rather to ensure that all users and management are fully aware of the rules surrounding the use of IT and to enable them to make safe and appropriate use of it.

Who does this guidance apply to?

This guidance applies to any authorised user of the Trust's systems or IT services (including users accessing remotely).

Users include: Teachers, support staff, Governors, volunteers, partner organisations, employees (utilising the School network), and contractors who directly or indirectly support or have access to the school's IT systems.

The School's Responsibilities

All schools within the Acorn Trust are responsible for ensuring that their systems and information are secure and any use of IT is reasonable and legitimate. The school therefore reserves the right to monitor, maintain and keep records to ensure compliance with this guidance.

Your responsibilities

All users have a responsibility to use these resources safely, securely, efficiently and in a professional and lawful manner. Users of the school's IT systems and services will be expected to have read and understood this Acceptable Usage Policy alongside the E-safety Policy, Mobile Phone Usage Policy and Social Media Policy.

Headteacher responsibilities

Responsibility for the enforcement of the guidance is the combined responsibility of all school employees and users and (if appropriate) their managers. Headteachers within the Trust need to ensure that this guidance is discussed with employees as part of their induction process and revisited on a regular basis.

1.1 Key definitions in this guidance

This guidance defines the Trust's view on what it considers to be acceptable, unacceptable and expressly forbidden use of IT.

At all times all employees must comply with the Trust's Staff Code of Conduct and with the law in their use of the school's IT.

Users should also comply with:

- E-safety Policy
- Social Media Policy
- Mobile Phone Usage Policy
- I-pad Acceptable Use Policy

Examples of acceptable, unacceptable and forbidden include, but are not limited to, the examples quoted in this Policy.

The definitions outlined below:

Acceptable
The activities listed as acceptable define the degree of flexibility that the Trust allows to all authorised users of IT. The Trust wants people to feel comfortable using new technologies and will help in their development in this key area.

Unacceptable
Users carrying out activities in this category will be regarded as in breach of the guidance and this may result in action under the Trust's disciplinary procedure. Unacceptable behaviour could also be classed as gross misconduct if significant enough, such as usage for long periods, persistent offender, several unacceptable activities taking place. This could ultimately lead to dismissal from employment.

Forbidden
Users carrying out activities in this category will be regarded as in breach of the guidance and this will be subject to action under the Trust's disciplinary procedure and may constitute gross misconduct where appropriate. This could ultimately lead to dismissal from employment. Users may also be subject to civil and criminal proceedings.

As a general guide, if there is any doubt about what is meant by acceptable, unacceptable or forbidden use for IT, you should seek advice from your Headteacher, IT support staff, School Business Manager or Chief Executive Officer (CEO).

2 Acceptable use of School IT systems and services

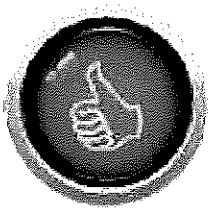
The following sections clearly outline what the Trust considers to be acceptable, unacceptable and forbidden use of the school's IT under the headings internet, e mail,

PCs, laptops and servers, user accounts and passwords and telephone (mobile and landline) use.

It is important to note that examples of acceptable, unacceptable and forbidden activities include, but are not limited to, those quoted in this Acceptable Usage Policy. Please read these alongside the E-safety Policy, Social Media Policy and Mobile Phone Usage Policy.

2.1 Use of internet services

The Trust's position on acceptable, unacceptable and forbidden use of the Internet is defined below:



Acceptable

- Accessing work related websites in relation to the user's job;
- Accessing non-work related web sites outside of your working hours. Any personal use must not include any activity outlined in the 'unacceptable' and 'forbidden' sections below.

Unacceptable

- Providing your work e-mail address as contact details to sites you have accessed for non-work purposes. This poses a greater potential security risk to the school's network by encouraging spam e-mails or chain e-mails;
- Accessing personal social media sites such as Facebook using school equipment
- Looking at non-work related internet sites such as Facebook at any time during the school day other than unpaid lunchtime.
- Using web based e-mail for example Facebook e-mails or Google mail (gmail) from your work equipment at any time;
- Downloading any copyright material without the owner's permission

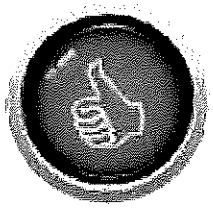
Forbidden

- Spending any excessive periods of the normal school day looking at non-work related internet sites;
- Downloading software used for hacking or cracking passwords without prior consultation with the IT service and CEO;
- Making repeated attempts to access websites that, because of their inappropriate content, have been automatically blocked by the school's web filtering software;
- Tying up internet resources on non-work related activity, to the detriment of genuine school internet usage. This includes:
  - leaving live internet feeds open to collect news or sports results;
  - downloading images, video or audio steams for non-business related purposes;
- Accessing sites containing pornographic, offensive, extremist, racist or obscene material that may cause offence to others;
- Using someone else's personal user account and password to access the internet;
- Attempting to circumvent or avoid any school security features.
- Staff must not allow pupils to use staff work spaces on any devices.

It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users

2.2 Use of e mail services

The Trust's position on acceptable, unacceptable and forbidden use of e mail is defined below:



Acceptable

- Communication in connection with school business;
- Management and Headteacher access to read employees or user's mail boxes where there is a legitimate need, authorised by the CEO or Headteacher, to do so (such as when a person is absent and an important e-mail is expected). This may require the school to access personal communications to you.

Unacceptable

- Excessive use of e-mail internally for personal non-business purposes;
- Use of school e-mail **externally** for non-school purposes;
- Forwarding chain emails;
- Sending work related information to and from your personal e-mail address without the permission of the Headteacher or CEO;
- Supplying your work e-mail address for non-business related activities for example Facebook, internet banking, ebay or high street stores;
- Sending business related e-mail directly to large distribution groups (such as parents of all pupils), without approval from the Headteacher / CEO.

Forbidden

- Sending messages or files that contain discriminatory, abusive, extremist, racist, pornographic, obscene, illegal, offensive, potentially libellous or defamatory content;
- Sending personal or sensitive school material to employees' personal e-mail accounts, or to unauthorised internal or external recipients;
- Sending e-mails from another user's account **unless specific approval or permission is obtained, which would be granted for example for specific shared mail box management;**
- E-mailing confidential, sensitive or personally identifiable information to other people (internal or external) without ensuring that this data is appropriately secured;
- Sending files with non-school related attachments (such as compressed files, executable code, video streams, audio streams, or graphical images) to internal or external parties;
- Using web based mail services such as Facebook mail or Google mail (gmail).

It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users

Note: Unsolicited receipt of discriminatory, extremist, abusive, pornographic, obscene, illegal, offensive, or defamatory e mail is clearly not a disciplinary offence, although anyone who receives such material should inform their Headteacher, whether it is from a known or unknown sender. The Headteacher should seek appropriate advice from the CEO.
If users receive offensive or pornographic material from a known sender, whether they are themselves offended by it or not, they should immediately and politely make the sender aware that they do not wish to receive any similar material. If the material comes from an unknown source, the message must be deleted without a message being sent back to the originator.

2.3 Use of PCs and laptops.

The Trust's position on acceptable, unacceptable and forbidden use of PCS, laptops and servers is defined below:

Acceptable

- Creating and storing data in connection with school business in a way which ensures that this data is regularly backed up. **Note:** laptops must be encrypted before business use and handheld devices password protected;
- Loading text images, video or audio streams in connection with normal school business.

Unacceptable

- Loading any unauthorised or untested software, such as software not purchased through the formal purchasing process. This includes, for example, software downloaded from internet web sites, whether freeware or commercially sold;
- Storing school data on the local drive of your PC or laptop, which is not subject to back up routines;
- Storing your own personal data on any school device including a memory stick, mobile phone, a school PC, laptop or server, such as music files, films, games, video clips, images;
- Leaving your PC, laptop or blackberry unattended without locking the machine or device (for PCs), password enabling (for handheld devices) or logging off.

Forbidden

- Loading files containing pornographic, offensive or obscene content, whether in text, image, video or audio format
- Use of unencrypted laptops for, mobile or electronic devices for school business; (See Mobile Phone Policy)
- Storing personal material which is protected by copyright, such as picture, music, video, games, etc. software that has **not** been purchased through formal school channels;
- Use of unencrypted or encrypted non-school issue mobile storage devices to store school data including school e-mails;
- Deliberate, reckless or negligent introduction of a virus into the school's IT;
- Installation and/or use of software with remote control

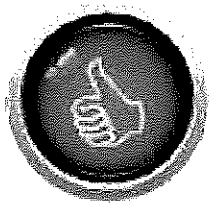
Consent;

- Storing school data that contains confidential, sensitive or personal information on the local drive of a PC, laptop or removable media such as CD, DVD or pen drive;
- Printing off any personally identifiable or sensitive information from school systems and sharing this with individuals who do not have the right to access or see this information;
- Not disposing of or storing paper documents containing personally identifiable or sensitive information in a safe, and approved confidential way.

It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users. The procedure for use of mobile devices is also available within the E-safety Policy, Social Media Policy and Mobile Phone Usage Policy.

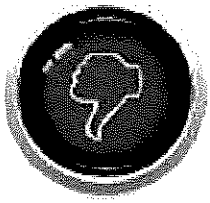
2.4 Use of user accounts and passwords

The Trust's position on acceptable, unacceptable and forbidden use of user network and application accounts, and passwords is defined below:



Acceptable

- Using your own, personally assigned user account to carry out your work at school;
- Using administrator accounts to carry out your daily tasks in response to specific administrator activities assigned to you by your manager;
- Access to other user accounts with the owner's explicit permission. This can only be granted where there is a legitimate business need and approval is required from the Headteacher or CEO.



Unacceptable

- Requesting the password for a user account assigned to another member of staff.

Forbidden

- Sharing a password associated with any user account assigned to you;
- Resetting the password associated with a user account assigned to someone else, without the owner's express permission;
- Providing the password for a user account personally assigned to another member of staff;
- Using a user account that has been provided to another member of staff without correct permission by the Headteacher or CEO;
- Using a session established by another user under their own personal account;
- Using a privileged user account to access data where there is no specific business reason to do so.

It is the user's responsibility to ensure their user account and password details are not disclosed. If there is any suspicion that your details are known then you should change your password. If you suspect your user account details have been used without authorisation notify the Headteacher immediately.

It is important to note that the above lists are not considered to be exhaustive but aim to provide clear guidelines for employees / users

2.5 Use of telephones (mobiles and landlines)

The Trust's position on acceptable, unacceptable and forbidden use of telephones is defined in the Trust's Social Media Policy and Mobile Phone Usage Policy.

It is important to note that it is the School Business Manager's responsibility to monitor usage of both landline and school mobile telephones and report any concerns to the Headteacher.

3 Monitoring

The Trust reserves the right to monitor and keep records of any use of its IT for a number of reasons relevant to the school's business, including but not limited to:

- ensuring compliance with this guidance and other related Trust guidance documents that the school has adopted;
- training and monitoring standards of service;
- ascertaining whether internal or external communications are relevant to the Trust's business;
- preventing, investigating or detecting unauthorised or criminal activities through the use of the school's IT;
- maintaining the effective operation of the school's IT system; and
- E-mails addressed to you which are received during your absence from work (such as sickness or holiday), may be reviewed by the Headteacher or nominated manager, where there is a legitimate need to do so, authorised by the Headteacher. This may inadvertently lead to the school accessing personal communications to you.

Authorised officers may occasionally need to undertake activities that fall into 'Unacceptable' or 'Forbidden' categories to carry out their daily work. This is acceptable provided that it is done with the full knowledge and agreement of the Headteacher.

The Trust fully appreciates that users have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy whilst in the work environment. However, all users should take note that our safeguarding software, Impero, will track words used in communication and website searches and will alert school of possible misuse, even if it is marked as private or personal.

The Trust may employ automated and manual monitoring techniques on many of their systems, including the following, to ensure continued availability of the services and enable usage trends to be identified.

- E mail recording, logging and filtering
- Call and text logging (including content)
- Web content and URL logging and filtering
- USB device monitoring
- Anti-virus protection
- Anti-hacking and anti-spy ware tools

IT Technical staff legitimately accessing users email will guarantee confidentiality except to the extent that is required to follow up breaches of guidance, to comply with court orders or to facilitate criminal or disciplinary investigations.

Ultimately, schools are responsible for data held on equipment provided and, therefore, must retain the right to monitor the content of such data for legal compliance.

4 Glossary of terms

A number of terms are used throughout the Acceptable Usage Policy that may need explanation. These terms are defined below to further aid understanding.

IT

IT refers to system and applications, internet, e-mail, mobile devices including telephones and Blackberry devices, landlines, cameras and personal computers and servers.

Offensive

It is not possible to provide a definitive, prescriptive list of 'offensive' material. However the following identifies examples of the type of material that does fall within the definition of offensive throughout the acceptable use guidance.

'Material that is defamatory, racist or discriminatory on grounds of religion, disability, gender or sexual orientation, or alternatively which is designed to harass, victimise or bully, cause pain or distress to individuals.'

Obscene

Literal definitions of 'obscene' describe material that is 'offensive, outrageous or repellent' or material that is 'designed to deprave or corrupt' the audience. For the purpose of this document, any material that will cause extreme offence to a Trust employee, pupil, parent, business partner or visitor will be considered obscene.

Compressed files

Compressed files are ordinary files that have been changed so that they take up less space than the original file. These files when uncompressed can become extremely large and take up large amounts of space on the workstation or server. Commonly used compression tools are widely available and create files with a name extension of .zip.

Executable code

An executable is a file that contains a program, that is, a particular kind of file that is capable of being executed or run as a program in the computer. An executable file usually has a file name extension of .bat, .com, or .exe.

Limited use

This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work.

An example would be a **limited** number of occasions, spread over a wide period of time, perhaps 1–3 occasions per week, for periods up to 10 minute each time, over a period of two months or more.

Excessive use

This is not prescribed and varies according to the amount of time which the employee has spent not undertaking their legitimate work.

An example would be in **excess** of 3 times per week, for periods of more than 10 minutes each time, over a monitored period of at least one month.

Session

A session is the state in which a computer is left such that an interaction with connected resources can take place unhindered. Sessions are normally defined by a log on and log off action, or unlocking and locking a workstation using ctrl/alt/del keys.

Removable Media

Removable media consists of USB or Firewire memory sticks, mobile phones with the ability to connect as external drives, I-pods or MP3/4 players, floppy discs, CD/DVD/Blue- ray media, cameras, or portable or removable hard drives.

Adequate Protection or Encryption

Confidential, sensitive or personal information must be protected or encrypted using complex passwords of at least 8 characters of which at least 1 must be of numeric value.

For advice on how to do this please contact the School Business Manager or IT Technical staff within school.

IT Policy Framework

Other IT user documents you need to be aware of include:

- E-safety Policy
- Mobile Phone Usage Policy
- Social Media Policy
- I-Pad Acceptable Usage Policy for Staff
- Child Protection and Safeguarding Policy
- Whistleblowing Policy