

### **11.1 ICT Acceptable Use Policy**

**The development of new technologies has become integral to the lives of children in today's society, where the internet, digital information and communication tools can stimulate discussion and promote creativity.**

**This policy is intended to ensure that:**

- **children and adults will be responsible users and stay safe while using the internet, other communication technologies and digital resources for educational, personal and recreational use,**
- **school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.**

**This policy covers pupils and staff. Although Pages 1 – 12 only apply to pupils; staff should familiarise themselves with the complete document.**

Cundall Manor School (CMS) will try to ensure that pupils and staff have good access to ICT to enhance their teaching and learning and will expect the pupils and staff to agree to be responsible users in return.

Pupils and their parents will be asked sign the ICT Code of Practice for Pupils on joining the school and again at the beginning of each academic year.

All staff will sign the ICT Code of Practice for Teachers and Adults on joining the school and again at the beginning of each academic year.

CMS uses the Sophos web filtering software. Sophos web filtering uses a true real-time web content filter; it performs live analysis and real-time categorisation of web pages to dramatically improve protection and security.

## Pupils' use of internet

- Use of the internet, including e-mail, is permitted as directed by the teacher for purposes of research and learning directly related to the curriculum.
- Pupils will not be permitted to introduce or download executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these can in some cases contain harmful viruses. This includes but is not limited to copying such files onto the PupilShared (M) drive, saving them to your Home Directory (Z) drive and running them from a USB Memory Stick.
- Pupils will not be permitted to introduce or download music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto the school network or the workstation may breach their copyright.
- The use of game-style activities should be monitored by the teacher (or member of staff in charge of the ICT suite) to determine suitability. Games which are not age appropriate contain violence, inappropriate language or behaviour demeaning to others are **not** permitted. Pupils are to follow any directions relating to gaming activity from the supervising member of staff.
- Accessing websites that contain content and images which are not age appropriate, ie. from a film, television programme or game deemed to be for older viewers, is not permitted.
- Images from the Internet are not to be accessed, downloaded or printed without prior permission from the supervising member of staff.
- Pupils are permitted to view online videos. They are to follow any directions relating to online video activity from the supervising member of staff.
- Personal e-mail, social networking or instant messaging sites are **not** permitted during school times. They will only be available during the week between 5pm and 10pm and weekends between 9am and 6pm.
- Children should report any misuse of the internet to their teacher.
- Pupils must not access websites that incite radicalisation or compromise the fundamental British values held by the school.
- Children should be made aware of the possibility of online bullying and the increasing threat of radicalisation via the Internet.
- When e-mail is required as part of a curriculum based lesson, **all** e-mails transmitted and received will be approved by teaching staff.
- No e-mail will be approved where it may include information that may offend others or where it does not respect the rights, beliefs and feelings of others. Pupils of CMS should always remember that they are representing themselves and our school.
- Personal information such as full names, home addresses, and phone numbers should **never** be sent by e-mail.
- We reserve the right to investigate incidents that take place outside school hours, on school visits and trips and that occur in the vicinity of the school, involving our pupils

## **Pupil use of the school network**

- All pupils will be given a user name to access the network. Pupils must log onto the school network using their personal user name only.
- Pupils must not work at or tamper with a station that has been logged on by another user, even for short periods of time.
- Pupils must only access information stored on the shared area pupilshared (M) drive or your personal Home Directory (Z) drive.
- Pupils must not edit or delete any information that is stored on the Shared Area.
- Pupils will ensure they log off after they have finished their session and leave the workstation in a tidy manner.
- Pupils will not use the network in any way that would disrupt the use of the network by others.
- Pupils will not introduce “USB drives” or other portable devices into the network without having them approved and checked for viruses by the ICT Manager.
- Pupils must not reveal their password to anyone, if they think that someone is using their logon details they must inform a teacher or contact the ICT Manager.

## **Cundall Manor School ICT Code of Practice for Pupils**

Dear Parents / Carers,

The internet is an amazing resource for us in school. It enables children to gain access to an unprecedented level of information. ICT allows your child access to a variety of interactive learning resources which stimulates both learning and creativity.

Unfortunately, the use of the internet is not without its dangers and some materials accessible through it are inappropriate for children. However, whereas no system can be guaranteed to be 100% safe, the huge benefits far outweigh the disadvantages and every reasonable precaution, including monitoring and filtering systems, are used to ensure that children will be safe when they use the internet and ICT systems.

Whilst the school monitors ICT use in school it needs to be understood that children also have an important responsibility themselves as to how they use the internet and school equipment.

**Please read through the ICT Code of Practice for your child, discuss the points and impress upon them how important these are.**

# Cundall Manor School

## Pupil Acceptable Use Policy (PP1 – Form 3)

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

<b>Computer Rules</b>	
1	I will only use polite language when using the computers.
2	I must not write anything that might upset someone or give the school a bad name.
3	I know that a member of staff will regularly check what I have done on the school computers.
4	I must not tell anyone my name, where I live, or my telephone number - over the Internet.
5	I must not tell my username and passwords to anyone else but my parents.
6	I must never use other people's usernames and passwords or computers left logged on by them.
7	I must log off after I have finished with my computer.
8	I know that any electronic message is not guaranteed to be private and could be forwarded without my knowledge.
9	I will report any websites that make me feel uncomfortable to a trusted adult.
10	I will tell my parents or a teacher straight away if I am sent any messages that make me feel uncomfortable.

11	I will not try to harm any equipment or the work of another person on a computer.
12	I will not attempt to download material that is not suitable for my age.

**Pupil User Agreement Form for the Pupil Acceptable Use Policy**

I agree to follow the school rules when using the school computers. I will use the network in a sensible way and follow all the rules explained by my teacher.

If I do not follow the rules, I understand that this may mean I might not be able to use the computers.

Pupil's Name: \_\_\_\_\_

Pupil's Signature: \_\_\_\_\_

I realise that any pupil under reasonable suspicion of not following these rules when using (or misusing) the computers may have their use stopped, more closely monitored or past use investigated.

Parent's Name: \_\_\_\_\_

Parent's Signature: \_\_\_\_\_

Date: \_\_/\_\_/\_\_\_\_

# Cundall Manor School

## Pupil Acceptable Use Policy (Form 4 – Form 6)

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

### Conditions of Use

Pupil access to the networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Pupils must also accept personal responsibility for reporting any misuse of the network to the IT Manager.

### Acceptable Use

Pupils are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All users however must think carefully about their actions and how they will affect the wider community. We recognise that personal electronic devices may be used to support learning, but they can also be disruptive when not used appropriately. Pupils are expected to accept personal responsibility when using electronic devices and should be aware that sanctions may be given if the device is used in a way that is at odds with the principles of the school community and that the school reserves the right to investigate and take appropriate disciplinary action in such circumstances.

The following list does provide some examples that must be followed:

1	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
---	--

2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I realise that files held on the school network can be regularly checked by the IT Manager or other members of staff.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6	I will work at my own computer and not deliberately interfere with the work of another pupil.
7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8	I will ensure that I log off after my network session has finished.
9	If I find an unattended machine logged on under another user's username I will not continue using the machine – I will log it off immediately.
10	I understand that I will not use social media or attempt to gain access to it while in school.
11	I am aware that an electronic message is not guaranteed to be private and that it can be forwarded without my knowledge. Messages that are supportive of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted.
12	I will not use the network in any way that would disrupt use of the network by others.
13	I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to a member of staff
14	I will scan any "USB drives" or other portable devices introduced to the network for viruses.
15	I will not attempt to visit websites or download material that might be considered inappropriate for my age or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	I will not attempt to download and/or install any unapproved software, system utilities or resources from the Internet.
17	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.
18	I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.

19	I will not bring a mobile phone or other electronic device into school or on any school trip unless specifically given permission by the member of staff in charge.
----	---

**UNACCEPTABLE USE**

- Examples of unacceptable use include, but are not limited to:
- Logging in with another person’s user ID and password, or using a machine left unattended, but logged in by another user.
- Creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person.
- Unauthorised access to data and resources on the school network system that belong to other “users”.
- User action that would cause:
  - Corruption or destruction of other users’ data,
  - Violate the privacy or dignity of other users,
  - Intentionally waste time or resources on the school network or elsewhere.

**NETWORK SECURITY**

If you discover a security problem, for example being able to access other user’s data, you must inform the IT Manager immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

**Pupil User Agreement Form for the Pupil Acceptable Use Policy**

I agree to follow the school rules on the use of the school network resources. I will use the network in a responsible way and observe all the conditions explained in the school acceptable use policy.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that students under reasonable suspicion of misuse in terms of time or content may have their usage monitored or their past use investigated.

Pupil Name: \_\_\_\_\_

Pupil Signature: \_\_\_\_\_

Parent Name: \_\_\_\_\_

Parent Signature: \_\_\_\_\_

Date: \_\_/\_\_/\_\_\_\_

# **Cundall Manor School**

## **Pupil Acceptable Use Policy (Leckby – Thornton)**

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems at risk and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

### **Conditions of Use**

Pupil access to the networked resources is a privilege, not a right. Pupils will be expected to use the resources for the educational purposes for which they are provided.

It is the personal responsibility of every student to take all reasonable steps to make sure they follow the conditions set out in this Policy. Pupils must also accept personal responsibility for reporting any misuse of the network to the IT Manager.

### **Acceptable Use**

Pupils are expected to use the network systems in a responsible manner. It is not possible to set a complete set of rules about what is, and what is not, acceptable. All users however must think carefully about their actions and how they will affect the wider community. We recognise that personal electronic devices may be used to support learning, but they can also be disruptive when not used appropriately. Pupils are expected to accept personal responsibility when using electronic devices and should be aware that sanctions may be given if the device is used in a way that is at odds with the principles of the school community and that the school reserves the right to investigate and take appropriate disciplinary action in such circumstances.

The following list does provide some examples that must be followed:

1	I will not create, send or post any material that is likely to cause offence or needless anxiety to other people or bring the school into disrepute.
2	I will use appropriate language – I will remember that I am a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3	I will not use language that could stir up hatred against any ethnic, religious or other minority group.
4	I realise that files held on the school network can be regularly checked by the IT Manager or other members of staff.
5	I will not reveal any personal information (e.g. home address, telephone number) about myself or other users over the network.
6	I will work at my own computer and not deliberately interfere with the work of another pupil.
7	I will not share my login details (including passwords) with anyone else. Likewise, I will never use other people's username and password.
8	I will ensure that I log off after my network session has finished.
9	If I find an unattended machine logged on under another user's username I will not continue using the machine – I will log it off immediately.
10	I understand that I will not use social media or attempt to gain access to it while in school.
11	I am aware that an electronic message is not guaranteed to be private and that it can be forwarded without my knowledge. Messages that are supportive of illegal activities will be reported to the authorities. Anonymous / unnamed messages are not permitted.
12	I will not use the network in any way that would disrupt use of the network by others.
13	I will report any accidental access to other people's information, unsuitable websites or being sent inappropriate materials that make me feel uncomfortable to a member of staff
14	I will scan any "USB drives" or other portable devices introduced to the network for viruses.
15	I will not attempt to visit websites or download material that might be considered inappropriate for my age or illegal. I am aware that downloading some material is illegal and the police or other authorities may be called to investigate such use.
16	I will not attempt to download and/or install any unapproved software, system utilities or resources from the Internet.
17	I will not receive, send or publish material that violates copyright law. This includes materials sent / received using Video Conferencing or Web Broadcasting.

18	I will not attempt to harm or destroy any equipment, work of another user on the school network, or even another website or network connected to the school system.
----	---

**UNACCEPTABLE USE**

Examples of unacceptable use include, but are not limited to:

- Logging on with another person’s user ID and password, or using a machine left unattended, but logged in by another user.
- Creating, transmitting, displaying or publishing any material (text, images or sounds) that is likely to harass, cause offence, inconvenience or needless anxiety to any other person.
- Unauthorised access to data and resources on the school network system that belong to other “users”.
- User action that would cause:
  - Corruption or destruction of other users’ data,
  - Violate the privacy or dignity of other users,
  - Intentionally waste time or resources on the school network or elsewhere.

**NETWORK SECURITY**

If you discover a security problem, for example being able to access other user’s data, you must inform the IT Manager immediately and not show it to other users. Students identified as a security risk will be denied access to the network.

**Pupil User Agreement Form for the Pupil Acceptable Use Policy**

I agree to follow the school rules on the use of the school network resources. I will use the network in a responsible way and observe all the conditions explained in the school acceptable use policy.

If I do not follow the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that students under reasonable suspicion of misuse in terms of time or content may have their usage monitored or their past use investigated.

Pupil Name: \_\_\_\_\_

Pupil Signature: \_\_\_\_\_

Parent Name: \_\_\_\_\_

Parent Signature: \_\_\_\_\_

Date: \_\_\_/\_\_\_/\_\_\_\_\_

## APPENDIX 1– Staff Only

### Use of mobile phones

- While it is recognised that members of staff may need to use their own telephone to contact each other, or relay information regarding expected arrival times from trips, any contact with parents or pupils should be undertaken through the school telephone system or using school mobile telephones, i.e. parents and pupils should not contact members of staff on their personal mobile phones. All calls to staff regarding school business should be directed through the main school telephone number.
- Staff must not use their own mobile telephones for taking photographs of children.
- Mobile phones should not be used when teaching, unless in an emergency.
- CMS has a number of mobile phones which are available for staff to use when on school trips. These phones are only to be used for pupil/ parent contact and emergency use.
- Pupils who bring mobile phones to school should only use them in case of emergency and should not use them during lesson times, unless otherwise indicated by the supervising member of staff.
- Mobile phones must not **by law** be taken into an EYFS setting
- Mobile phones must not **by law** be used while driving

## Staff use of internet

- Use of the internet on school premises should principally be for school use, e.g. accessing learning resources, educational websites, researching curriculum topics, use of e-mail on school business.
- Use of the school's internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is prohibited.
- The school recognises that information can now be accessed online through the 'streaming' of data, i.e. radio, television, music, etc. Teachers and administration staff should only access streamed information if it is of educational interest to a lesson or to its planning. For example, using BBC iPlayer is acceptable if it is in the interest of the class and related lessons. Streaming music for personal use is discouraged. This is due to the streaming process placing demands on the schools internet bandwidth; as a result the internet can become slow for all users. Streaming data for personal use is not authorised.
- Teachers should not be accessing the internet for personal reasons whilst teaching children.
- Use of the internet to access any illegal sites or inappropriate material is a disciplinary offence. If accessed accidentally users should report the incident immediately to one of the Joint Heads or IT Manager, so the incident can be logged.
- Staff should not use any school computer to access social networking sites, such as Facebook, Twitter, etc, due to the potential virus risk these sites can carry. Any damage caused to school computer equipment as a result of such misuse is the responsibility of the member of staff, who may be asked to compensate the school.
- The school recognises that many staff will actively use Facebook, Twitter, and other such social networking sites, blogging and messaging services. Staff must not post material (including text or images) which damages the reputation of the school or which causes concern about their suitability to work with children. Staff must recognise that it is not appropriate to post information or discuss issues relating to children or other members of staff via these networks. Those who post material which could be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct.
- Staff should be aware of the latest Teachers Standards available here: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/283566/Teachers\\_standard\\_information.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/283566/Teachers_standard_information.pdf)
- Any photos or videos taken during **any** school activity should not be put on public display or published anywhere on the internet (including social networking sites such as Facebook) unless for school promotional purposes and with regard to pupils for whom the parents have given permission.
- It is **never** acceptable to accept a 'friendship request' from pupils at the school. In almost all such cases the pupils will be breaching the terms and conditions of use of those networks and the member of staff will be compromising themselves in respect of Child Protection Procedures. It is also extremely inadvisable to accept as friends ex-pupils who are still minors. If a parent of a pupil seeks to establish contact, the member of staff should exercise their professional judgement at all times.
- Setting a high security level on social networking sites as advisable.

- Staff must not access websites that incite radicalisation or compromise the fundamental British values held by the school.
- Staff must log onto the school network using their personal user name and password only. Staff must not access the school network using the administrator user name and password or any other user name.
- Staff must not download software onto the school network before first liaising with the IT Manager to check for suitability. Software that is installed and is deemed not necessary for use in the school context will be deleted, i.e. iTunes, mobile telephone software, games, etc.
- Staff must ensure they log off after they have finished their session and leave the workstation in a tidy manner.
- Staff will ensure that they lock their workstation if left unattended to avoid unauthorised access to staff drives or school e-mails.
- Staff will not use the network in any way that would disrupt use of the network by others.
- Staff should not introduce “USB drives” or other portable devices into the network without having them approved and checked for viruses by the ICT Manager.
- School resources, such as software, etc. are for the use of staff and pupils within the school premises only and should **not** be taken home for personal use.

### **Use of portable computer systems, USB sticks or any other removable media**

- If sensitive data, such as children’s details and report comments, is stored on a portable device it should be encrypted or password protected. Other data, such as lesson plans and resources, may be stored on unencrypted devices.
- Staff should ensure all data is stored and used in compliance with the DPA 1998.

### **Use of digital images**

- Any photos or videos taken by teachers, other adults (including parents), and the children themselves during ANY school activity (including educational visits) should not be put on public display or published anywhere on the internet (including social networking websites).
- The above excludes the publication of photos on the CMS website, within the school newsletter, for the purpose of school related publicity, and where used by the school for educational/display uses, where the parents have given express permission to the school for them to do so.

### **Use of school hardware – laptops, cameras, recording equipment, etc.**

- Use of school laptops, cameras, video cameras and recording equipment is limited to activities directly related to school activity. They can be used during lessons, sporting activities, school visits and residential trips. They are not for personal use.
- All data must be transferred to the school network as soon as possible to ensure that data is saved and protected. Once copied to the network the data must be deleted from the recording equipment.
- If travelling with these hardware items, and they contain information relating to staff and pupils, i.e. address details, photographs or reports, ensure that files are encrypted and password protected.

Reviewed September 2018

**NOTE**

**It should be understood by all staff, that this Code of Practice is in place to protect staff from potential risk in their use of ICT in their everyday work and to protect the school network.**



# CUNDALL MANOR SCHOOL

## ICT Acceptable Use Policy

### Cundall Manor School ICT Code of Practice for Teachers and Adults

**I confirm that I have read and understood the Acceptable Use Policy (including those aimed at pupils) for ICT and agree to abide by it.**

**Signed**

---

**Print**

---

**Date**

---