



# The Linden Centre

## ICT & Acceptable Use Policy

Signed by:		
	Headteacher	Date:
	Chair of Management Committee	Date

Last Updated	04 <sup>th</sup> January 2021
Review Due:	04 <sup>th</sup> January 2022

## Contents:

1. <i>Introduction</i>	3
2. <i>Purpose</i>	3
3. <i>Scope</i>	5
4. <i>Safe use of technology</i>	7
5. <i>Procedures</i>	7
6. <i>Unacceptable Usage</i>	9
7. <i>Sanctions</i>	10
8. <i>Key Principles and Rules</i>	11
9. <i>Appendix 1</i>	0
10. <i>Appendix 2</i>	2
11. <i>Appendix 3</i>	6
12. <i>Appendix 4</i>	8
13. <i>Appendix 5</i>	9

## 1. Introduction

- 1.1. The Linden Centre is committed to protecting its pupils, from illegal or damaging use of technology by individuals, either knowingly or unknowingly.
- 1.2. As users of the School's IT services pupils have a right to use its computing services; that right places responsibilities on these users which are outlined below. Misuse of the computing facilities in a way that constitutes a breach or disregard of the following policy may also be in breach of other School policies.
- 1.3. Ignorance of this policy and the responsibilities it places on users is not an excuse in any situation where it is assessed there has been a breach of the policy and its requirements.
- 1.4. Pupils are directed to this policy during their induction and are required to acknowledge their agreed adherence to and compliance with the policy when they first log on to the network.

## 2. Purpose

- 2.1. The purpose of this policy is to:
  - 2.1.1. outline the acceptable and unacceptable use of computer equipment or "online services" owned by the School, and acceptable or unacceptable general behaviour in ICT areas;
  - 2.1.2. educate and encourage pupils to make good use of the educational opportunities presented by access to technology;
  - 2.1.3. safeguard and promote the welfare of pupils, in particular by anticipating and preventing the risks arising from:
    - exposure to harmful or inappropriate material (such as pornographic, racist, extremist or offensive materials);
    - the sharing of personal data, including images;
    - inappropriate online contact or conduct; and
    - cyberbullying and other forms of abuse;
  - 2.1.4. help pupils take responsibility for their safe use of technology (i.e. limiting the risks that children and young people are exposed to when using technology);

- 2.1.5. ensure that pupils use technology safely and securely and are aware of both external and peer to peer risks when using technology.

- 2.2. These rules are in place to protect pupils and the School. Inappropriate use exposes the School and its Partners to risks including virus attacks, compromise of network systems and services, and legal issues.

### **3. Scope**

- 3.1. This policy applies to all pupils within The Linden Centre.
- 3.2. The School will take a wide and purposive approach to consider what falls within the meaning of technology. This policy relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them including:
- the internet
  - email
  - mobile phones and smartphones
  - desktops, laptops, netbooks, tablets/phablets
  - personal music players
  - devices with the capability for recording and / or storing still or moving images
  - social networking, microblogging and other interactive web sites
  - instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
  - webcams, video hosting sites (such as YouTube)
  - gaming sites
  - Virtual Learning Environments
  - Interactive Whiteboards
- 3.3. This policy applies to the use of technology on School premises.
- 3.4. This policy also applies to the use of technology off school premises if the use involves pupils or any member of the School community or where the culture or reputation of the School or a member of staff is put at risk.



## 4. Safe use of technology

- 4.1. We want pupils to enjoy using technology and to become skilled users of online resources and media. We recognise that this is crucial for further education and careers.
- 4.2. The School will support pupils to develop their skills and make internet access as unrestricted as possible whilst balancing the safety and welfare of pupils and the security of our systems. Pupils are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.
- 4.3. Pupils may find the following resources helpful in keeping themselves safe online:
  - <http://www.thinkuknow.co.uk>
  - <http://www.childnet.com>
  - <http://www.childline.org.uk/Pages/Home.aspx>

## 5. Procedures

- 5.1. Pupils are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be safe, responsible, respectful to others and legal. If a pupil is aware of misuse by other pupils, he/she should talk to a teacher about it as soon as possible.
- 5.2. Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Prevention of Bullying policy. If a pupil thinks that he/she might have been bullied or that another person is being bullied, he/she should talk to a teacher about it as soon as possible. See the School's Prevention of Bullying policy for further information about cyberbullying and online safety, including useful resources.
- 5.3. In many cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures. If a pupil is worried about something that he/she has seen on the internet, or any electronic device, including on another person's electronic device, he/she must tell a teacher about it as soon as possible.
- 5.4. In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported

to the Designated Safeguarding Lead and the Headteacher who will record the matter centrally.

## 6. Unacceptable Usage

- 6.1. The School provides internet access to pupils to support their academic progress and development.
  - 6.1.1. Unacceptable use of School technology and network resources may be summarised as, but not restricted to: Actions which cause physical damage to any ICT hardware, including peripherals (eg, mouse, cables, wiring, printers);
  - 6.1.2. Creating, displaying or transmitting material that is fraudulent or otherwise unlawful, likely to cause offence or inappropriate;
  - 6.1.3. Viewing, retrieving, downloading or sharing any offensive material which may include abusive content, racist, considered to be of an extreme or terrorist-related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity;
  - 6.1.4. Threatening, intimidating or harassing staff, pupils or others;
  - 6.1.5. Intellectual property rights infringement, including copyright, trademark, patent, design and moral rights;
  - 6.1.6. Defamation;
  - 6.1.7. Unsolicited advertising often referred to as "spamming";
  - 6.1.8. Sending emails that purport to come from an individual other than the person sending the message using, e.g., a forged address;
  - 6.1.9. Not adhering to the acceptable data storage levels set by the Director of ICT;
  - 6.1.10. Attempts to break into or damage computer systems or data held thereon;
  - 6.1.11. Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software, eg use of equipment which is inadequately protected against viruses and spyware;
  - 6.1.12. Attempts to access or actions intended to facilitate access to computers for which the individual is not authorised;

- 6.1.13. Using the School network for unauthenticated access;
  - 6.1.14. Any other conduct which may discredit or harm the School, its staff, community or the ICT Facilities;
  - 6.1.15. Using the ICT facilities for gambling;
  - 6.1.16. Using the ICT facilities for carrying out any illegal trading activity.
- 6.2. This policy sets out the following rules and principles with which pupils must comply:
- Authorisation - access and security
  - Use of the internet and email
  - Use of mobile electronic devices and
  - Photographs and images.
- 6.3. These principles and rules apply to all use of technology.
- 6.4. Anyone who mistakenly accesses inappropriate material should notify ICT Support.
- 6.5. The School may inform the police or other law enforcement agency in the event of any use that could be regarded as giving rise to criminal proceedings.

## **7. Sanctions**

- 7.1. Where a pupil breaches any of the School rules, practices or procedures set out in this policy or the appendices, the School may apply any sanction which is appropriate and proportionate to the breach including, in the most serious cases, expulsion. Other sanctions might include increased monitoring procedures and withdrawal of the right to access the School's internet and email facilities. Any action taken will depend on the seriousness of the offence.
- 7.2. Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with the practices and procedures in this policy.

## 8. Key Principles and Rules

### 1 Authorisation - access and security

- 1.1 Any attempt to access or use any user account or email address, for which the pupil is not authorised, is prohibited.
- 1.2 Pupils may not use or attempt to use, ICT resources allocated to another person, except when explicitly authorised.
- 1.3 Pupils must take all reasonable precautions to protect the School's resources (including the ICT Facilities and the School's information and data), their username and passwords.
- 1.4 Purpose of Use
  - 1.4.1 ICT facilities are provided primarily to facilitate a person's essential work as a pupil. Use for other purposes, such as personal email or recreational use of the Internet, is only permitted during the permitted times specified by the School and is a privilege, which can be withdrawn at any time and without notice. Any such use must not interfere with the pupil's studies or any other person's use of computer systems and must not, in any way, bring the School into disrepute.
  - 1.4.2 School email addresses and associated School email systems must be used for all official School business.
- 1.5 The School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of pupils. Pupils must not try to bypass this filter.
- 1.6 Viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. Pupils must not disable or uninstall anti-virus software on the School's computers.
- 1.7 Privacy and Monitoring
  - 1.7.1 All allocated usernames, passwords and email addresses are for the exclusive use of the individual to whom they are allocated. Pupils are personally responsible and accountable for all activities carried out under their username. The password associated with a particular personal username must not be divulged to any other person.
  - 1.7.2 Passwords should not be recorded where they may be easily obtained and should be changed immediately if it is suspected that they have become known to another person.
  - 1.7.3 For the protection of all pupils, their use of email and the internet

when accessed via the School network will be monitored by the School. Pupils should remember that even when an email or something that has been downloaded has been deleted, it can still be traced on the system. Pupils should not assume that files stored on servers or storage media are always private

- 1.7.4 Pupils must not interfere or attempt to interfere in any way with information belonging to or material prepared by another user. Similarly, pupils must not make unauthorised copies of information belonging to another user. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.

## 2 Use of the internet and email

### 2.1 Use of the internet

- 2.1.1 Pupils must take care to protect personal and confidential information about yourself and others when using the internet, even if the information is obtained inadvertently
- 2.1.2 Pupils must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, abusive content, racist, considered to be of an extreme or terrorist-related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. Pupils must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.
- 2.1.3 Pupils must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.
- 2.1.4 Pupils must not bring the School into disrepute through their use of the internet.
- 2.1.5 Copyright Compliance
- 2.1.5.1 All pupils must abide by by-laws relating to the use and protection of copyright.
- 2.1.5.2 Pupils must not download, copy or otherwise reproduce the material for which they have not obtained permission from the relevant copyright owner. If such material is required for any purpose eg research then copyright permission must be obtained and documented before such material is used.

2.1.5.3 Pupils are reminded that the School treats plagiarism very seriously and will investigate any allegation i.e. the intentional use of other people's material without attribution.

### 3 Use of mobile electronic devices

- 3.1 "Mobile electronic devices" includes but is not limited to mobile 'phones, smartphones, tablets, laptops and MP3 players.
- 3.2 Pupils are not permitted at any time to connect devices with a network cable in any part of the School or to any other school Wi-Fi network.
- 3.3 All children may bring a mobile phone to school if they travel to school independently, but they must leave it at the School Office during the School day.
- 3.4 Pupils must not communicate with a member of staff's personal (as opposed to School) mobile phone except when this is expressly permitted by a member of staff (e.g., if a staff member has no school mobile and communication, is required for the normal running of School business). For example, this may on occasion be necessary during an educational visit. Any such permitted communications should be brief and courteous.
- 3.5 Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not they are in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use and the School's safeguarding procedures will be followed in appropriate circumstances.
- 3.6 Mobile electronic devices may be confiscated in appropriate circumstances. Pupils may also be prevented from bringing a mobile electronic device into the School temporarily or permanently.
- 3.7 The School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed into staff.

## 4 Photographs and images

- 4.1 Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- 4.2 Pupils may only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- 4.3 Pupils must allow staff access to images stored on mobile phones and / or cameras and must delete images if requested to do so.
- 4.4 The posting of images which in the reasonable opinion of the School is considered to be offensive or which brings the School into disrepute on any form of social media or websites such as YouTube etc is a serious breach of discipline and will be subject to disciplinary procedures whatever the source of the material, irrespective of whether the image was posted using School or personal facilities.

### **4.5 Sexting (Youth Produced Sexual Imagery)**

- 4.5.1 'Sexting' means the taking and sending or posting of images or videos of a sexual or indecent nature, usually through mobile picture messages or webcams over the internet.
- 4.5.2 Sexting is strictly prohibited, whether or not the pupil is in the care of the School at the time the image is recorded and / or shared.
- 4.5.3 Sexting may also be a criminal offence, even if the picture is taken and shared with the permission of the person in the image.
- 4.5.4 Remember that once a photo or message is sent, you have no control about how it is passed on. You may delete the image but it could have been saved or copied and may be shared by others.
- 4.5.5 Images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.
- 4.5.6 The School will treat incidences of sexting (both sending and receiving) as a breach of discipline and also as a safeguarding matter under the School's child protection procedures (see the School's Child Protection and Safeguarding Policy and procedures).
- 4.5.7 If you are concerned about any image you have received, sent or forwarded or otherwise seen, speak to any member of staff for advice.

## 5 Responsibilities

- 5.1 This policy is the responsibility of the ICT Subject Lead.
- 5.2 The ICT Subject Lead is responsible for ensuring that issues around data protection and copyright compliance are monitored.
- 5.3 All School Managers are responsible for the implementation and monitoring of the policy.
- 5.4 The responsibility for the supervision of the Acceptable Use Policy is delegated to ICT Support by the School Executive. Any suspected breach of this policy should be reported to a member of the ICT Support staff. A responsible senior member will then take the appropriate action within the School's disciplinary framework; other members of the School ICT Support staff will also act when infringements are detected in the course of their normal duties. All incidents involving the safe use of technology will be logged.
- 5.5 The Designated Safeguarding Lead will consider the record of incidents and logs of internet activity as part of the ongoing monitoring of safeguarding procedures.
- 5.6 Consideration of the efficiency of the School's online safety procedures and the education of pupils about keeping safe online will be included in The Management Committee' annual review of safeguarding.

## 9. Appendix 1

### 1.1 ICT Services Acceptable Use Policy (AUP) Summary for Pupils

- 1.1 You must not:
  - 1.1.1 Allow other people to use your account.
  - 1.1.2 Download or access illegal software onto a workstation.
  - 1.1.3 Download or copy any software packages from the School network onto portable media, etc.
  - 1.1.4 Upload your software packages onto a School workstation.
  - 1.1.5 Access offensive or abusive material.
  - 1.1.6 Send or receive offensive, abusive or inappropriate e-mails.
  - 1.1.7 Access "inappropriate" websites - some Internet pages are illegal and may be subject to criminal proceedings.
  - 1.1.8 Interfere with other users' work.
  - 1.1.9 Photograph or record members of staff or pupils without their permission, using devices such as mobile phones, cameras or digital recorders.
  - 1.1.10 Use software designed to unblock sites.
  - 1.1.11 Use online gambling sites.
  - 1.1.12 Use peer-to-peer and related applications anywhere on school premises.
  - 1.1.13 Abuse equipment.
  - 1.1.14 Make offensive or inappropriate comments including bringing the School's name and reputation into disrepute on any forum/platform, such as social media sites (whether using a school device or not) where a connection between the user and The Linden Centre can reasonably be made.
- 1.2 Please remember, when in teaching and learning areas such as open areas or classrooms:
  - 1.2.1 Keep noise to a minimum to avoid disrupting others.
  - 1.2.2 Copyright regulations apply to electronic sources - please check before you print out from online services.
  - 1.2.3 No unauthorised use of chat rooms.
  - 1.2.4 Logout or lock your computer when leaving a computer, even for a short time.

- 1.2.5 Be able to show a certificate showing that any portable electrical device (such as your personal laptop/power supply etc) has been electrically tested, before using it on School premises.
- 1.3 Anyone found abusing the School policy on the use of computers may have their network rights removed and may be subject to further disciplinary action.
- 1.4 School computers are provided primarily for Schoolwork. However, you may use the equipment for personal use providing:
  - 1.4.1 You do not breach the Acceptable Use Policy.
  - 1.4.2 You are not doing so for gambling purposes.
- 1.5 If you use the School equipment for personal use, you should note the following:
  - 1.5.1 Conducting any financial transaction on shared equipment carries a very high risk. Your personal data may not be safe.
  - 1.5.2 This Acceptable Use Policy applies to both wired and wireless access and use of the network on your own equipment or on School equipment.
  - 1.5.3 In order to use the ICT facilities of the School, you must first be properly registered to use such services.
- 1.6 Pupils are not permitted to connect their device directly via cable to any network socket within the organisation or to any other Wi-Fi network that the school transmits.
- 1.7 The school reserves the right to remove access at any time. Pupils must abide by all of this policy when their device is connected to the school network.

## 10. Appendix 2

### 1.2 ICT Services Acceptable Use Policy (AUP) Summary for Staff

- 1.1 Covers use of digital technologies in school: i.e. email, internet, intranet and network resources, learning platform, software, equipment and systems.
  - 1.1.1 I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Management Committee.
  - 1.1.2 I will not reveal my password(s) to anyone.
  - 1.1.3 I will follow 'good practice' advice in the creation and use of my password (to include upper case, lower case, number and special characters). If my password is compromised, I will ensure I change it. I will not use anyone else's password if they reveal it to me and will advise them to change it.
  - 1.1.4 I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
  - 1.1.5 I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
  - 1.1.6 I will always log off a computer when I am not using it. I will never leave a computer logged on.
  - 1.1.7 I will not engage in any online activity that may compromise my professional responsibilities or reputation.
  - 1.1.8 I will only use the approved, secure email system(s) for any school business.
  - 1.1.9 I will only use the approved school email or other school approved communication systems with pupils or parents/carers, and only communicate with them on appropriate school business.
  - 1.1.10 I will ensure that my personal devices NEVER automatically synchronise with any school endorsed system (except email), particularly where images from personal devices can be uploaded to school network spaces.
  - 1.1.11 I will not browse, download or send material that could be considered offensive to colleagues.
  - 1.1.12 I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager / school named contact.
  - 1.1.13 I will not download any software or resources from the Internet that can compromise the network, or are not adequately

licensed.

1.1.14 I will not publish or distribute work that is protected by copyright.

- 1.1.15** I will not connect a computer, laptop or other device to the network / Internet that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's recommended antivirus, firewall and other ICT 'defence' systems. 33 Online safety policy April 2017
- 1.1.16 I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- 1.1.17 I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role, e.g. NOT making references to school, staff, pupils or parents on Facebook, posting pictures from school or pupils on Facebook, posting videos from school on YouTube, 'friending' pupils or parents of pupils on Facebook (this list is not exhaustive).
- 1.1.18 I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- 1.1.19 I will access school resources remotely (such as from home) only through office 365/ school approved methods and follow online security protocols to access and interact with those materials.
- 1.1.20 I will only use OneDrive as a means to store and share information that is not confidential or does not contain personal information, e.g. photos of students, student records, etc.
- 1.1.21 I will ensure that I follow school data security protocols when using any confidential data transported from one location to another.
- 1.1.22 I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- 1.1.23 I will alert a Designated Safeguarding Lead if I feel the behaviour of any child in the school may be a cause for concern.
- 1.1.24 I understand that it is my duty to support a whole-school safeguarding approach and will report any behaviour (of other staff or pupils), which I believe may be inappropriate or concerning in any way, to a senior member of staff/DSL at the school.
- 1.1.25 I understand that failure to comply with this agreement could lead to disciplinary action.
- 1.1.26 (Teaching staff only): I will embed the school's online safety curriculum into my teaching.

## Acceptable Use Agreement: Staff

### User Signature

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent e-safety policies.
- I wish to have an email account; be connected to the school network, email & internet; be able to use the school's ICT resources and systems.

Signature .....Date.....

Full Name ..... (printed)

Job title .....

Authorised Signature (Online Safety Coordinator)

I approve this user to be set-up.

Signature ..... Date.....

Full Name ..... (printed)

## 11. Appendix 3

### 1.3 ICT Services Acceptable Use Policy (AUP) Summary for Parents/Carers

#### 1.1 Internet and ICT

1.1.1 As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my daughter/son access to:

- the internet at school;
- ICT facilities and equipment at the school.

1.1.2 I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials.

1.1.3 I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school, and if there are concerns about my child's e-safety or online behaviour they will contact me.

#### 1.2 Use of digital images, photography and video

1.2.1 I understand the school has clear guidelines on the use of digital images and video and I support this.

1.2.2 I understand that the school may use photographs of my child or including them in video material to support learning activities, and that my permission will be sought on entry to the school.

1.2.3 I accept that the school may want to use photographs/video that include my child in publicity that reasonably promotes the work of the school, and for no other purpose, and that my permission will be sought on entry to the school.

1.2.4 I will not take and then share online, photographs of other children (or staff) at school events without permission.

#### 1.3 Social networking and media sites

1.3.1 I understand that the school has clear guidelines on the use of social networking and media sites, and I support this.

1.3.2 I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour.

1.3.3 I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns.

1.3.4 I will be mindful of the school reputation when on social media.

1.3.5 I know that I can see a copy of the school's online safety policy on request.

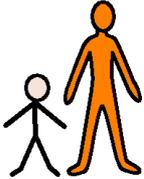
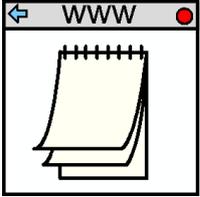
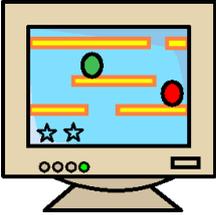
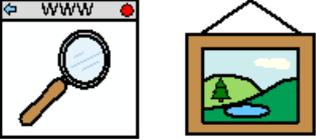
1.3.1 My child's name(s): \_\_\_\_\_

1.3.2 Parent / guardian name: \_\_\_\_\_

1.3.3 Parent / guardian signature: \_\_\_\_\_ Date: \_\_\_\_\_

## 12. Appendix 4

### 1.4 Acceptable Use Agreement: Pupils (Primary)

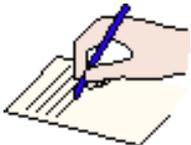
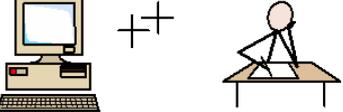
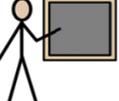
	<p>No phones at school</p>
	<p>Only use the computer if you are with an adult.</p>
	<p>Use kids' websites only. No social media.</p>
	<p>Only play kids' games. Nothing too old for you.</p>
	<p>Be careful what you search for online.</p>
 <p>Tell an adult if something is worries you online</p>	

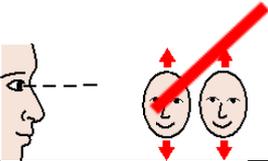
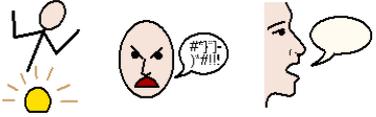
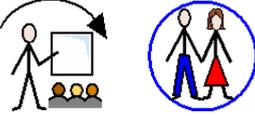
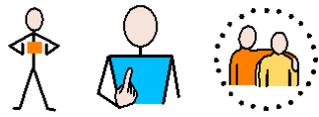
Signed (Student) \_\_\_\_\_ Date \_\_\_\_\_

Signed (Parent/Carer) \_\_\_\_\_ Date \_\_\_\_\_

### 13. Appendix 5

#### 1.5 Acceptable Use Agreement: Pupils (Secondary)

	<p>I cannot use the school's ICT equipment until my parents/carers and I have signed this online safety agreement.</p>
	<p>I will not give out personal/private information online.</p>
	<p>I will never call or meet anyone in person that I've met online unless my parents/carers approve and agree to go with me.</p>
	<p>I can only use the school's computers and ICT equipment for my school work.</p>
	<p>If I am not sure whether I am allowed to do something on the computers I will ask a member of staff.</p>
	<p>I will only use <b>my</b> username, and I will not share my password.</p>
	<p>I will not use the internet or mobile phones to be mean rude or hurtful to anyone.</p>
	<p>I will only go on the internet at school when a teacher has given permission and is present.</p>
	<p>I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell a trusted adult straight away.</p>

<p>1.5.1</p> 	<p>While at school I will not try to search for things online that I know are not acceptable.</p>
	<p>If I find anything mean, rude, or things that I know are not acceptable I will immediately report it to my teacher.</p>
	<p>The online safety rules apply to any ICT devices brought into school.</p>
	<p>I will treat all ICT equipment/devices with care and respect.</p>
	<p>I will not download or install software on school technologies.</p>
	<p>I will teach my parents/carers about the internet, and let them know exactly what I am doing when I am online.</p>
	<p>I understand that these rules are designed to keep me, and my family and friends safe.</p>

**Signed (Student)** \_\_\_\_\_  
**Date** \_\_\_\_\_

**Signed (Parent/Carer)** \_\_\_\_\_  
**Date** \_\_\_\_\_

