Halstead CP School

Acceptable Use Policy

Approved by the Full Governing Body

Signed :

Patricia Dunmall (Chair of Governors) – Mr Hawkins (Headteacher)

Date : May 2017
To be reviewed : May 2019

CONTENTS

Introduction

The Acceptable Use Policy has been agreed by all members of the school community and builds on the KCC Acceptable Use Policy and government guidance.

At Halstead Community Primary School we encourage and support the positive use of Information and Communication Technology (ICT) to develop both formal and informal learning opportunities in school. We carefully manage the use of ICT and online tools to ensure that all members of the school community are kept safe as well as their data and that risks or dangers are recognised and mitigated.

1. Information for staff, visitors and volunteers

With internet use becoming more prominent in everyday life for both personal and professional use, it is important that all members of staff are made aware that their online conduct both in and out of school could have an impact on their role and reputation. Civil, legal or disciplinary action could be taken should staff be found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All adults who work within the school either as employees or volunteers (including all teaching, non-teaching staff, volunteers, PTA groups, Governors etc.) must be aware of the school rules and expectations for use of school information systems and professional conduct online whether on or off site. Misuse of ICT systems and other professional misconduct rules for employees (whether from Kent County Council or other professional bodies) are specific and instances resulting in disciplinary procedures or staff dismissal have occurred.

2.1 Advice for staff

At Halstead Community Primary School, we encourage staff, volunteers and visitors to avoid the use of personal email and social networking, such as YouTube, Facebook and Twitter as it can leave staff vulnerable to abuse or a blurring of professional boundaries. Although we would not ban staff from using social networking sites in your own personal time, contact with pupils and parents (past or present) should only take place via school approved and provided communication channels, e.g. school email address, so it can be monitored and traced in the case of an allegation or concern. All staff should ensure that any contact between staff and pupils and parents takes place within clear and explicit professional boundaries and be transparent and open to scrutiny at all times.

However, in some cases there may be pre-existing or external relationships. If this is the case, staff are expected to make a member of SLT of these exceptions in order to protect themselves from allegations or misinterpreted situations.

Staff are advised to regularly review their privacy settings on any personal social media sites they use, however it should be remembered that once content is shared online it is possible for it be circulated more widely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared).

Staff must appreciate that school systems must be safeguarded from misuse and any activity on school devices and systems could be checked if required. Any online behaviour and activity by a member of staff whilst using the school systems must be in accordance of the school AUP and any policies relating to staff conduct and personal use must not interfere with the member of staff's duties or be for commercial purpose or gain (unless authorised by the leadership team/managers).

Staff should read and sign the Staff Acceptable Use Policy appendix 1.

2.2 Information for visitors and volunteers

At Halstead Community Primary School, we encourage staff, volunteers and visitors to avoid the use of personal email and social networking, such as YouTube, Facebook and Twitter as it can leave visitors/volunteers vulnerable to abuse.

It's important that any visitors or volunteers are aware of the Acceptable use Policy as it an important tool to safeguard the community.

Visitors and volunteers should read and sign the Visitor/Volunteer Acceptable Use Policy appendix 2.

2. Information regarding Children and Young People

At Halstead Community Primary School, we aim to ensure that the children are protected and are educated about safe and appropriate online behaviour. Children and young people should be empowered and supported to take responsibility for their own use of new technologies. We aim to enable children to use a range of technologies safely and responsibly.

With internet use an essential feature of children and young people's everyday life, we make them aware that their online conduct both in and out of school could have an impact both within and outside of school. Criminal, civil or disciplinary action could be taken, depending upon the child's age and the circumstances of the wrong committed.

In order to protect children, we have a Pupil AUP in view in the ICT suite and the content is discussed discussed with children on a regular basis as well as when they are actually using technology. Safe and positive online behaviour that is appropriate to their age and ability is embedded across the curriculum.

At Halstead Community Primary School we do not allow the use of personal devices (such as mobile phones) by pupils on-site. Any online behaviour and activity by a pupil should be in accordance with the school AUP and behaviour policy and comply with the law at all times.

All pupils are made aware that their internet and technology use may be recorded or monitored for safety and security reasons prior to internet or technology access.

Children are expected to sign an Acceptable Use Policy on entering the school which remains valid for the period of time that the child attends the school.

3. Information regarding parents/carers

The school will take every effort and all reasonable precautions to ensure that children cannot access inappropriate or illegal content whilst using the internet via school provided systems (including school provided Wi-Fi), however this cannot always be possible due to the dynamic nature of the internet.

The school has expectations of online conduct for the whole school community. Parents/carers are expected to support the school's approach to online safety (e-Safety) by not uploading, sharing or adding any pictures, video or text that could upset, offend or threaten the safety of any member of the school community.

The pupil AUP is shared with parents/carers in order to develop a cohesive approach to online safety (e-Safety) as children and young people use technology as part of everyday family life. We recognise that it is important that parents/carers are aware of the schools online safety (e-Safety) ethos and are actively engaged in supporting the school.

Parents/carers are expected to read the AUP with their child and sign to acknowledge the policy when their child starts attending the school. The Acceptable Use Policy then remains valid for the period of time that their child attends the school.

Appendix 1

Halstead Community Primary School
Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any images or videos of pupils will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the Staff Shared documents or KLZ SharePoint to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media

websites and the supervision of pupils within the classroom and other working spaces.

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Headteacher) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead (Headteacher) as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead (EIS) as soon as possible.

13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Headteacher).

18. I understand that my use of the school information systems (including any devices provided by the school), school Internet and school email may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of emails in order to monitor policy compliance. Where it believes unauthorised and/or inappropriate use of the schools information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the school suspects that the school system may be being used for criminal purposes then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

Accepted by: ……. Print Name: …….

Appendix 2

Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff who do not access school ICT systems

As a professional organisation with responsibility for children's safeguarding it is important that all members of the community are fully aware of their professional responsibilities and read and sign this Acceptable Use Policy. This is not an exhaustive list and visitors/volunteers are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

2. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentially, data protection and use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead (Headteacher).

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Headteacher) as soon as possible.

I have read and understood and agree to comply with the Visitor /Volunteer Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……

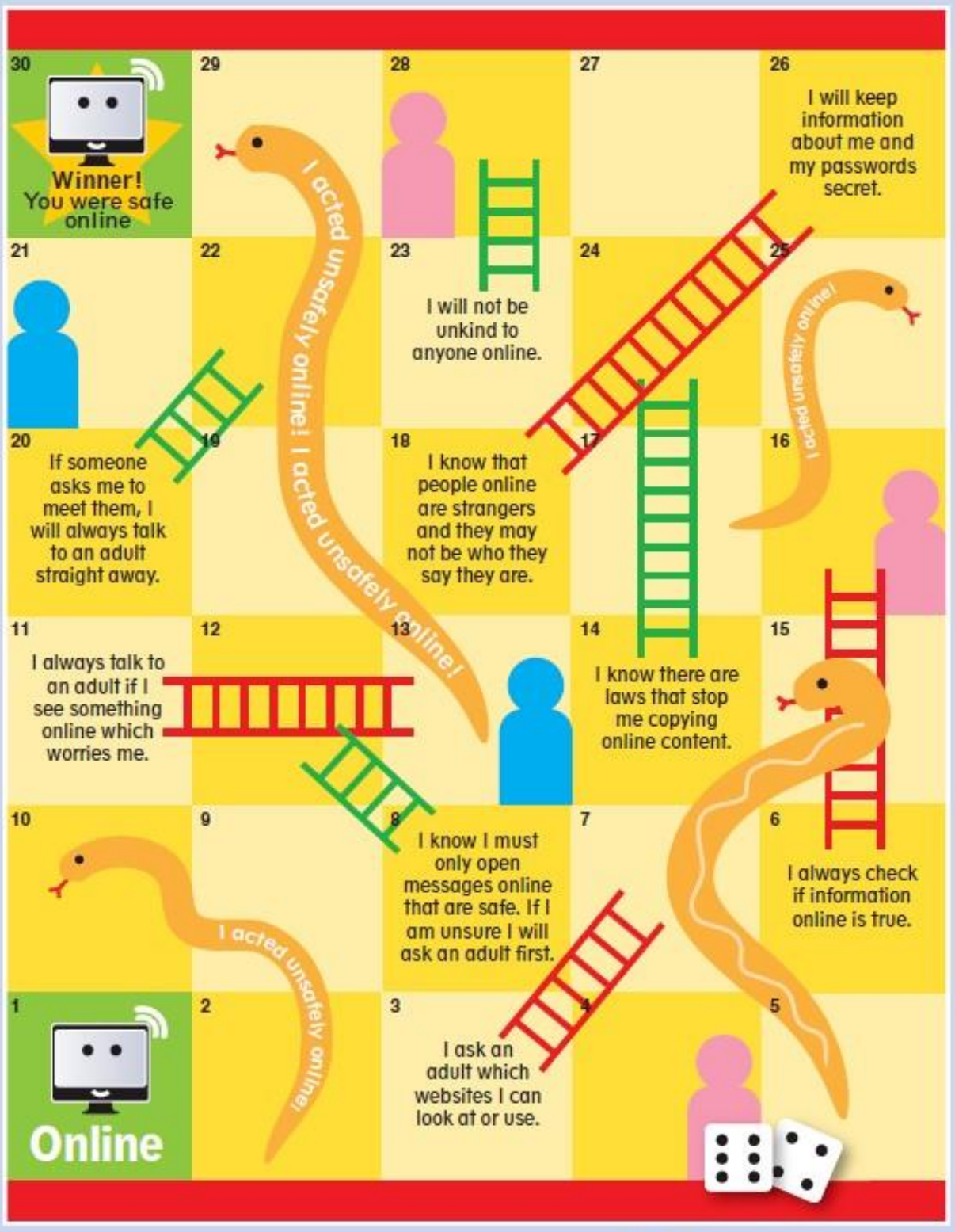
Accepted by:…… ……Date: ……..

Appendix 3

Early Years and KS1 Acceptable Use Poster

Appendix 4

KS2 Acceptable Use Poster



Halstead Community Primary School

Appendix 5

Pupil Acceptable Use Policy/e-Safety Rules

EYFS and Key Stage 1

These rules will help us stay safe on the Internet:

- I only go online with a grown up
- I am kind online
- I keep information about me safe online
- I tell a grown up if something online makes me unhappy or worried

Key Stage 2

These rules will help us stay safe on the Internet:

- I ask an adult which websites I can use
- I will not assume information online is true
- I know there are laws that stop me copying online content
- I know I must only open online messages that are safe and if I'm unsure then I won't open it without speaking to an adult first
- I know that people online are strangers and they may not always be who they say they are
- If someone online suggests meeting up then I will always talk to an adult straight away
- I will not use technology to be unkind to people
- I will keep information about me and my passwords private
- I always talk to an adult if I see something which makes me feel worried

Halstead Community Primary School

Appendix 6

Pupil Acceptable Use Policy/e-Safety agreement

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

Pupil:	Class:

Pupil's Agreement

- I have read and I understand the school e-safety rules.
- I can be trusted to use school ICT systems in a responsible manner.
- I know that network and internet access may be monitored.

Signed:	Date:

Parent's Consent for web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the Acceptable Use Policy and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from the use of Internet facilities.

Signed:	Date:
Please print name:	

Please complete, sign and return to the school office

Halstead Community Primary School

Appendix 7

Parent/Carers Acceptable Use Policy

- I have read and discussed the Acceptable Use Policy (attached) with my child
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted
- I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the schools behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school Online Safety (e-Safety) Coordinator (Mr Hawkins), my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety)
- I will visit the school website (www.halstead.kent.sch.uk) for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home

I have read the Parent Acceptable Use Policy.

Child's Name…… Class……

Parents Name…….....Parents

Signature…… Date…….

Note: Please be aware that if parents/carers refuse to sign and agree the AUP then this can cause issues as children will need to use the internet in order to access the curriculum.

Halstead Community Primary School

Appendix 8

Social Networking Acceptable Use Policy

For parents/volunteers running school/setting social media accounts e.g. PTA groups and committees

1. As part of the school's drive to encourage safe and appropriate behaviour in the use of today's technology, I will support the school's approach to online safety (e-Safety). I am aware that social media sites are public and global communication tools and that any content posted on them may reflect on the school, its reputation and services. I will not use the social media sites to express any personal opinions or create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring the school into disrepute.
2. I will not disclose information, make commitments or engage in activities on behalf of the school without authorisation from the school Designated Safeguarding Lead, Mr Hawkins (or Mrs Saheed/Mrs Troth in his absence). The head teacher (or other member of the leadership team) retains the right to remove or approve content posted on behalf of the school. Where it believes unauthorised and/or inappropriate use of social media or unacceptable or inappropriate behaviour may be taking place, the school will exercise the right to ask for the content to be deleted or deactivated.
3. I will ensure that any content posted abides by copyright and intellectual property rights, child protection legislation, privacy and data protection law and other relevant civil and criminal legislation.
4. I will follow the school's policy regarding confidentially and data protection/use of images. I will ensure that I have written permission from parents/carers or the school before using any images or videos which include members of the school community. Images of pupils will be taken on school equipment by the school and in accordance with the school image policy. Images which include pupils will only be uploaded by the school and these will be for the sole purpose of inclusion on the PAFA Facebook pages or the school Twitter account and will not be forwarded to any other person or organisation.
5. I will promote online safety in the use of social media and will help to develop a responsible attitude to safety online and to the content that is accessed or created.
6. I will set up a specific account/profile using a school provided email address to administrate the site and I will use a strong password to secure the account. The school Designated Safeguarding Lead and/or school management team will have full admin rights to the account.
7. I will ensure that the content and channel is suitable for the audience and will be sensitive in the tone of language used and will ensure content is written in accessible plain English.
8. I will report any accidental access or receipt of inappropriate materials or inappropriate comments to the Designated Safeguarding Lead, Mr Hawkins (or Mrs Saheed/Mrs Troth in his absence) immediately.
9. I will ensure that the (tool using e.g. Facebook, Twitter) is moderated on a regular basis as agreed with the Designated Safeguarding Lead, Mr Hawkins (or Mrs Saheed/Mrs Troth in his absence).
10. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices and the safe use of social media. I have ensured that the site has been suitably risk assessed and this use has been agreed by the head teacher.
11. If I have any queries or questions regarding safe and acceptable practise online I will raise them with the Designated Safeguarding Lead, Mr Hawkins (or Mrs Saheed/Mrs Troth in his absence).

I have read and understood and agree to comply with the School Parent Association Social Networking Acceptable Use policy.

Signed: ……... Print Name: …… Date: ……

Accepted by: …… Print Name: ……