Houghton Conquest
Pre-School

Houghton Conquest
Lower School
Growing together

Houghton Conquest Lower School and Pre School

Acceptable Use Policy and Agreements
(Staff, Volunteers, Governors and Pupils)

CONTENTS

Acceptable Use Policy

Introduction

At Houghton Conquest Lower 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.

We have an acceptable use policy for staff, volunteers and governors and one for pupils. Staff will sign the agreement *(see appendix 1)* during their induction. Pupils and parents will sign their agreement when they start school *(see appendix 3 & 7)* and again at the start of Key Stage 2 *(see appendix 5).*

Houghton Conquest Lower School provides a range of ICT resources which are available to all staff. In order to ensure the safety of both staff and pupils, it is important that all staff follow the guidelines detailed below.

This policy applies to all staff of the school, regardless of their use of ICT systems

School Email

Each member of staff and governors are provided with a school email address. The email system can be accessed from both the school computers, and via the internet from any computer. Wherever possible, all school related communication must be via the school email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the school does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school/setting business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- When sending emails all efforts should be made to not contain children's full names either in the subject line or the main body of the text. Initials should be used wherever possible.
- Access to school /setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the online safety incident file.
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Email sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- School email accounts will not be set up on personal mobile telephone devices, with the exception of the headteacher and school business manager as appropriate.

Internet Access

The school provides internet access for all staff and pupils in order to allow access to the wide range of content available. The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to the Online Safety Co-ordinator (School Business Manager). All members of staff need to understand that that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.

Supervision of pupils will be appropriate to their age and ability.

- At Early Years Foundation Stage and Key Stage 1 pupils' access to the Internet will be by adult demonstration or directly supervised access to specific and approved online materials which supports the learning outcomes planned for the pupils' age and ability.
- At Key Stage 2 pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary. Children will be directed to online material and resources which support the learning outcomes planned for the pupils' age and ability.
- It is not permitted to attempt to access, on any device, pornographic, illegal, sexist, violent, racist or inappropriate material in school.
- The use of live chat rooms is not permitted.
- The use of online real-time chat rooms is banned.

Digital cameras and iPad's

The school encourages the use of digital cameras, IPad's and video equipment; however staff should be aware of the following guidelines:

- Photos should only be named with the pupil's name if they are to be accessible in school only.
- Photos for the website or press must only be used if written permission is given by the parent/carer.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones and other tablets.
- All photos should be downloaded to the school network.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff will not be used for such purposes.
- Care should be taken when taking digital / video images that children / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Each member of staff must check the suitability and age appropriate content when downloading app's onto IPad's for pupils to use.

Security

Each member of staff is allocated a username and password. Staff are responsible for ensuring their password remains confidential and their account is secure. Staff will follow the guidelines below;

- Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.
- When any computer is left unattended, it must either be logged off, switched user or locked. No member of staff may use a computer which is found logged on as someone else - it must be immediately logged off.
- Staff will only access areas of the school's computer systems to which they have authorised access.

Communicating

Each member of staff will communicate online in a professional manner and tone, they will not use aggressive or inappropriate language and appreciate that others may have different opinions.
Members of staff will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
Members of staff are aware that any communication could be forwarded to an employer or governors.

File Storage

Each member of staff has access to shared network drives. Any school related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Removable media/storage devices are prohibited. No school data is to be stored on a home computer.

Remote Learning
During remote learning:

- I will not behave any differently towards students compared to when I am in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a pupil. The same applies to any private/direct communication with a pupil.
- I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- I will not take secret recordings or screenshots of myself or pupils during live lessons.
- I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom / impossible to tell that it is a bedroom if this is unavoidable (e.g. even if the camera slips). The camera view will not include any personal information or inappropriate objects and where possible to blur or change the background, I will do so.
- I will complete the issue log for live lessons if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of pupils.
- I understand that in past and potential future remote learning and lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.

ICT Acceptable Use Agreement: Pupils
Houghton Conquest Lower School provides a range of ICT resources which are available to pupils to help them learn and access the best online information to support their learning.

- We want pupils to use the ICT facilities safely, and with respect for themselves and other users.
- We want pupils to tell us if they have a problem and we will help to put it right.
- We hope that all our ICT users will develop safe practices that show respect for all other users.
- This policy applies to all school-provided ICT equipment and to pupils' uses of ICT whether in school or not, and whether they occur inside or out of normal school hours.

Internet Access
The school provides internet access for all pupils in order to allow access to the wide range of content available to support learning.

- The school's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on rare occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website should be *immediately* reported to the class teacher by the pupil. The teacher will report it immediately to the Online Safety Coordinator.
- Pupils will have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Pupils should always be reminded of using safe searches when using the internet.
- No pupil is permitted to share any personal information with anyone on the internet unless specific permission is given by the class teacher.

Social Networking
Houghton Conquest Lower School recognises the rise in popularity of social networking sites, and the rapid development of sites specifically targeted at primary aged children.

- Pupil's must not attempt to contact any members of staff or request to be 'friends' with them through any social networking site or personal email service.
- Pupils must not post derogatory comments about Houghton Conquest Lower School staff, governors or pupils on social media sites.
- Parents should not contact staff regarding any school issue via a social networking site. All contact must be made through the school.
- 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 morewidely than intended without consent or knowledge (even if content is thought to have been deleted or privately shared).

- Please refer to our Social Media Policy.

Linked Policies
Online Safety Policy
Safeguarding Policy
Social Networking Policy
GDPR Policy
Data Breech Policy

Appendix 1

Houghton Conquest Lower 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. I will protect the devices in mycare from unapproved access or theft.

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 ormore 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 legislation (including GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longerthan necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely (e.g. via VPN).

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.

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's online safety policy which covers the requirements for use of mobile phones and personal devices and safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of learners within the classroom and other working spaces.

11. I will immediately report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the School Business Manager and Designated Safeguarding Lead 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 and the School Business Manager 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 Designated Safeguarding Lead.

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 local authority, 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 Online Safety Coordinator or the Designated Safeguarding Lead.

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.

19. I understand that the school may exercise its right to monitor the use of information systems, including internet access and the interception of emails, to monitor policy compliance. Where it believes unauthorised and/or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation

20. I understand that if I use my personal computing equipment for school business that I will have fully active and up to date antivirus software and appropriate device security installed at all times.

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

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

Appendix 2

Visitor/Volunteer Acceptable Use Policy

For visitors/volunteers and staff

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 useshould be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

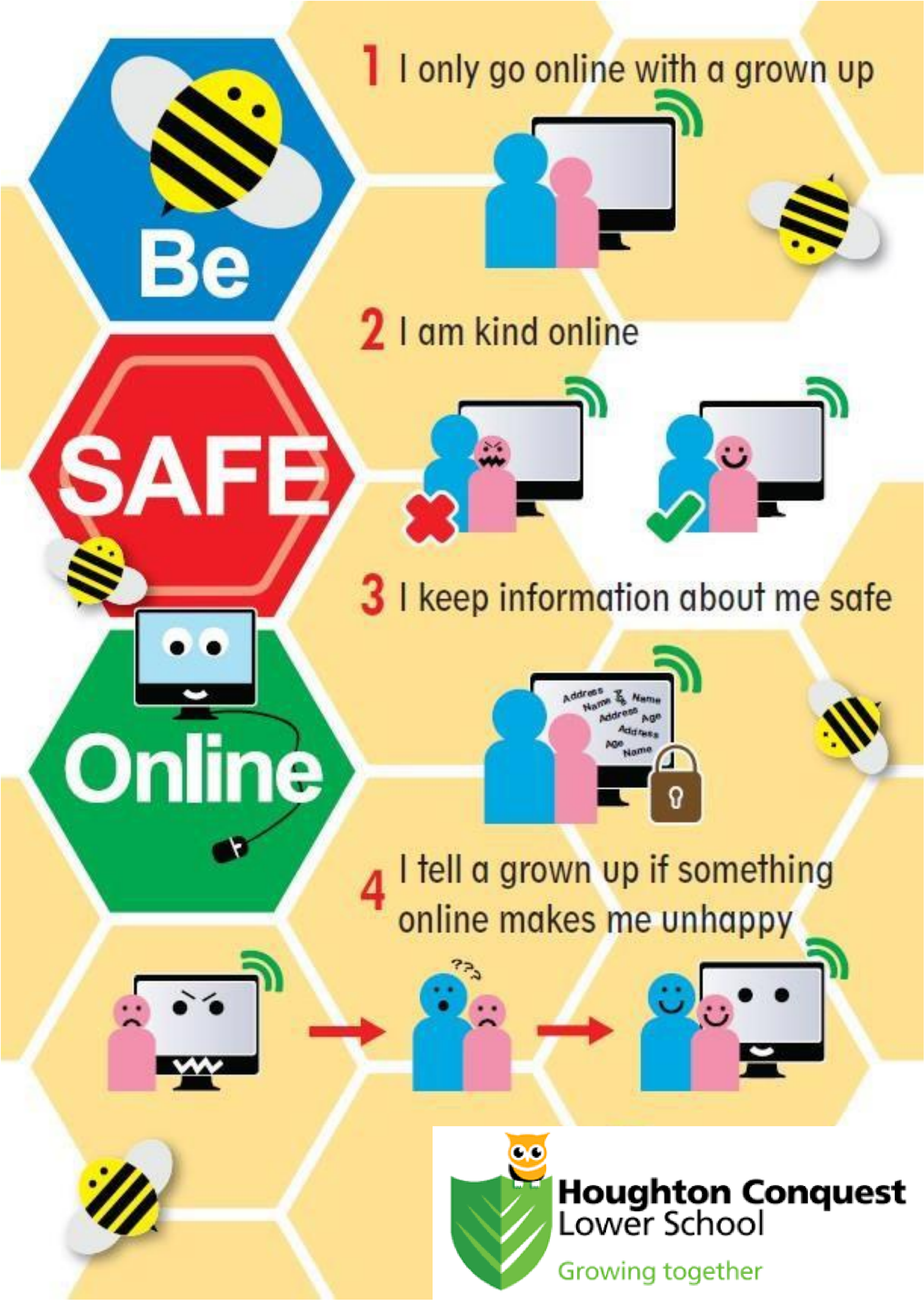
1. I will ensure that any personal data of learners, staff or parents/carers is kept in accordancewith Data Protection legislation, including GDPR. Any data which is being removed from thesite, such as via email or on memory sticks or CDs, will be encrypted by a method approvedby the setting. Any images or videos of learners will only be used as stated in the school image use policy and will always reflect 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 mediawebsites 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 imagesand 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 opento scrutiny at all times. All communication will take place via school approved communicationchannels e.g. via a school provided email address or telephone number and not via personaldevices 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 Designated Safeguarding Lead or the School Business Manager.
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 bringmy professional role, the school, or the local authority, 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 Online Safety Coordinator or the Designated Safeguarding Lead.
9. I will report any incidents of concern regarding children's online safety to the Online Safety Coordinator or the DesignatedSafeguarding Lead as soon as possible.
10. I understand that if the school believes inappropriate use or unacceptable behaviour is taking place, the school may invoke its disciplinary procedure. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation.
11. I understand that if I use my personal computing equipment for school business that I will have fully active and up to date antivirus software and appropriate device security installed at all times.

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

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

Appendix 3

Early Years and KS1 Acceptable Use Poster



Be SAFE Online

1 I only go online with a grown up

2 I am kind online

3 I keep information about me safe

4 I tell a grown up if something online makes me unhappy

Appendix 4

Pupil’s ICT Agreement/e-safety Rules

KS 1 / Reception

Pupil’s Name: ……………………………………………………….

- ✓ I will ask an adult before using the computers, laptops and ipads/tablets
- ✓ I will follow the instructions of the teacher when using them
- ✓ I will not give my full name, home address, telephone number, any other personal information or arrange to meet anyone under any circumstances
- ✓ I will tell my teacher if I see anything on the computer which I think I shouldn’t have done
- ✓ I am kind online
- ✓ I will tell an adult if something online makes me unhappy or worried
- ✓ I can be trusted to use the school ICT systems in a responsible manner.
- ✓ I know that network and internet access may be monitored.

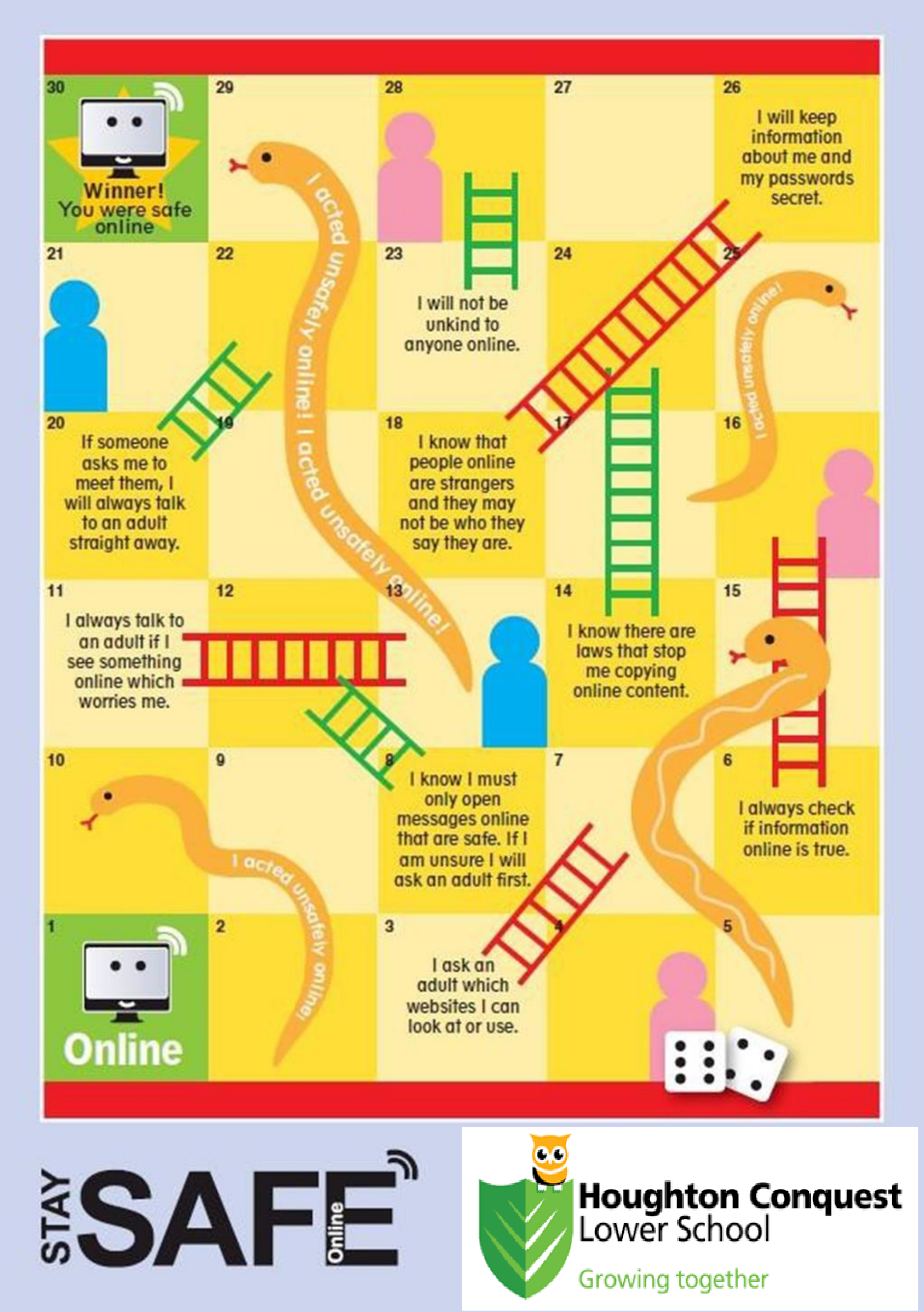
Parent’s Agreement

- ✓ I have discussed the above with my child
- ✓ I have read and accept the School’s Acceptable Use Policy

Signed …………………………………………… Date…………………….

Name *(please print)* …………………………………………….

Appendix 5
KS2 Acceptable Use Poster



Winner! You were safe online

I will keep information about me and my passwords secret.

I will not be unkind to anyone online.

If someone asks me to meet them, I will always talk to an adult straight away.

I know that people online are strangers and they may not be who they say they are.

I always talk to an adult if I see something online which worries me.

I know there are laws that stop me copying online content.

I know I must only open messages online that are safe. If I am unsure I will ask an adult first.

I always check if information online is true.

I ask an adult which websites I can look at or use.

Online

Appendix 6

Pupil's ICT Agreement/e-safety Rules

KS2

I agree that:

- ✓ I will always have permission from a member of staff before using the internet.
- ✓ I will not give my full name, home address, telephone number, any other personal information or arrange to meet anyone who tries to contact me under any circumstances.
- ✓ I will report any unpleasant material or messages sent to me, to my teacher immediately.
- ✓ I will not use technology to be unkind to people
- ✓ I know that people online are strangers and that they may not always be who they say they are.
- ✓ I will always talk to an adult if I see something which makes me feel worried.
- ✓ I can be trusted to use the school ICT systems in a responsible manner.
- ✓ I know that network and internet access may be monitored.

Pupils Name …………………………………………………. Class…………………….

Signed …………………………………………………………… Date…………………..

Parent's Agreement

I have read and accept the Schools Acceptable Use Policy and have discussed the policy with my child.

Signed …………………………………………………………… Date…………………..

Name *(please print)* …………………………………………….

Appendix 7

Parent/Carers Acceptable Use Policy

- I have read and discussed the attached Pupil's ICT Agreement/e-safety rules 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 andout of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- 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 willbe 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 Coordinator, my child's teacher or the Headteacher if I have any concernsabout online safety (e-Safety)
- I will visit the school website (www.hcschool.org.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……………