THE ASHBY FEDERATION

E-SAFETY POLICY

Approved by:	Executive Head Teacher
Last reviewed on:	December 2020
Next review due by:	December 2021

1. What is an E-safety Policy?

An E-safety Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones and games) to safeguard adults and children and young people within the school setting. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school setting. It also explains procedures for any unacceptable or misuse of these technologies by adults or children and young people.

In September 2020, the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE). KCSIE is statutory guidance from the DfE; all schools and colleges must comply with it when carrying out their duties to safeguard and promote the welfare of children.

The summary of key aspects related to online safety are as follows:
• All staff should undergo safeguarding and child protection training (including online safety) at induction
• The updated guidance includes a section (Part 5) on child on child sexual violence and sexual harassment, which can occur both on and offline
• Online safety is specifically referenced as part of the responsibility for the DSL within Annex B and directly referred to in Annex C.
• There is an expectation that DSLs will access appropriate training to ensure they are able to understand the unique risks associated with online safety, can recognise the additional risks that children with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe whilst they are online.

2. Why have an E-safety Policy?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies.
These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also vital that adults working or volunteering in the school are clear about the procedures and that the school complies with KCSIE 2019.

Whilst the school acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people continued to be protected.

3. Aims

- To ensure the safeguarding of all children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of all adults and children in the school setting.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. Roles and responsibilities of the school

4.1 Governors and Executive Headteacher

It is the overall responsibility of the Executive Headteacher, with the Governors, to ensure that there is an overview of E-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Executive Headteacher has designated an E-Safety Leader to implement agreed policies, procedures, staff training, and curriculum requirements. This person will take the lead responsibility for ensuring E-Safety is addressed in order to establish a safe ICT learning environment.

- Time and resources will be provided for the E-Safety Leader and staff to be trained and update policies, where appropriate.

- The Executive Headteacher is responsible for promoting E-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.

- The Executive Headteacher will report the progress of, or any updates to, the E-Safety curriculum (via PSHE or ICT) at the Safeguarding Committee Meetings and ensure Governors know how this relates to child protection.

At the Full Governor meetings, all Governors will be made aware of e-Safety developments from the Safeguarding meetings.

- The Governors must ensure Child Protection is covered with an awareness of e-Safety and how it is being addressed within the school, as it is the responsibility of Governors to ensure that all Child Protection guidance and practices are embedded.

- An E-Safety Governor (can be the ICT or Safeguarding Governor) will challenge the school about having an E-safety Policy with appropriate strategies which define the roles, responsibilities for the management, implementation and safety for using ICT, including challenging the school about having:
    - Firewalls
    - Anti-virus and anti-spyware software
    - Filters
    - Using an accredited ISP (Internet Service Provider)
    - Awareness of wireless technology issues
    - A clear policy on using personal devices.

- Ensure that any misuse or incident has been dealt with appropriately, according to policy and procedures and appropriate action is taken (see the Whistle Blowing and Child Protection Policy). See appendices for example procedures on misuse.

4.2 E-Safety Leader

It is the role of the designated e-Safety Leader to:

- Ensure that the E-safety policy is reviewed annually, with up-to-date information available for all staff to teach E-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff, children and young people, in the initial set up of a network, stand-alone PC or staff/children laptops and to ensure the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Executive Headteacher on a regular basis.
- Liaise with the DSL, DDSL and PSHE and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct E-safety information can be taught or adhered to.
- Update staff on the use of personal equipment in school:

    - Only school cameras are to be used in school or on school trips.
    - Personal memory sticks will not include any individual pupil data or images and will be encrypted (See GDPR Policy).
    - Images stored on school cameras, computers or school iPads will not be used at home.
    - Personal mobiles to be switched off during lesson times and out of sight of children
- Ensure that the ICT technician is directed to check for viruses on laptops, stand-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

4.3 Staff and adults

It is the responsibility of **all** adults within the schools to:

- Ensure that they know who the DSL, DDSL is within school so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Executive Headteacher. In the event of an allegation made against the Executive Headteacher, the Chair of Governors must be informed immediately (Whistle Blowing and Safeguarding Policy and Guidance on dealing with allegations of abuse against teachers and other staff)
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Executive Headteacher immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level. Report any concerns to the e-safety Leader.
- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Monitor the teaching of E-safety within the schools.
- Be up-to-date with E-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the GDPR policy.
- Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Report accidental access to inappropriate materials to the e-Safety Leader.

- Use anti-virus software and ask the ICT technician to check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies in accordance with the Safeguarding and Anti-bullying policies.

4.4 Children and young people

Children and young people are:

- Responsible for following the Internet Safety Rules whilst within school as agreed in the e-safety acceptable use Rules letter signed by parents/careers and children.
- Taught to use the Internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without reprimand (age and activity dependent).

5. Appropriate use by staff or adults

- Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources.
- This policy and any subsequent amendments will be discussed and agreed by all staff at a full staff meeting.
- The acceptable use should be similar for staff to that of the children and young people so that an example of good practice can be established.
- Please refer to appendices for agreed Internet Safety Rules for Staff.
- Appropriate use of mobile technologies is in the Staff Code of Conduct signed by all staff and regular volunteers.

5.1 In the event of inappropriate use

If a member of staff is believed to misuse the Internet in an abusive or illegal manner, a report must be made to the Executive Headteacher immediately who will then follow the procedures outlined in the Managing Allegations against Staff and the Safeguarding Policy.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

6. Appropriate use by children and young people

Internet Safety Rules and the letter for children and young people and parents/carers are outlined in the Appendices. The appropriate rules will be clearly displayed in each classroom and reinforced through curriculum teaching.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.
The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.
File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free.

6.1 In the event of inappropriate use

Should a child or young person be found to misuse the on-line facilities whilst at school the child or young person will be dealt with according to the 'Staff Procedures Following Misuse by Children and Young People' found in the appendices.

In the event that a child or young person accidentally accesses inappropriate materials, the child will report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the establishment.
Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

7. The curriculum and tools for Learning

7.1 Internet use

We teach our children and young people how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PSHE lessons. The following concepts, skills and competencies will have been taught by the time they leave Year 6.

- Internet literacy
- Making good judgements about websites
- Access to resources that outline how to be safe and responsible when using any on-line technologies
- File-sharing and downloading illegal content
- Uploading information – know what is safe to upload and not upload personal information.
- Where to go for advice and how to report abuse.
- Appropriate communication via social media.

We teach Internet use and safety through ICT lessons and PSHE and we use the www.thinkuknow.co.uk resources for KS1 and KS2. All E-safety teaching is recorded.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner.
Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have accidentally accessed something.

We ensure information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a parent/carer and should only contain something that would also be acceptable in 'real life'. Images of children and young people should be stored according to the GDPR policy.

7.2 Mobile phones and other technologies

- Children will not use mobile phones in school.
- Staff will switch off mobile phones during lesson times
- The use of staff mobile phones will be allowed for school trips for emergency use only.
- Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances.
- The use of mobile phones is detailed in the Staff Code of Conduct signed by all staff and regular volunteers.

7.3 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to school iPads and video cameras. These are the only cameras to be used in school.
Each class will have a school iPad but these will only be used on the direction of the staff within that classroom.
Images taken of children will only be stored within the school environment.

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website.
Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. gym kit.

8. Filtering and safeguarding measures

Anti-virus software is used on all network and stand alone PCs or laptops and is updated on a regular basis as agreed with the ICT technician.

Filtering is in place for all devices used in school as in maintained and checked by the ICT technician.

A firewall ensures information about our children and young people and the school cannot be accessed by unauthorised users.

Children use a search engine that is age appropriate and always monitored by a member of staff.

For older children and young people, they will be instructed to immediately turn the monitor off and report the inappropriate content viewed in error to another adult.

9. Parents

9.1 Roles

Each child or young person will receive a copy of the Acceptable Use Rules which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules.

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

School will keep a record of the signed forms.

9.2 Support

We will hold Parent/Carer Information sessions to deliver key messages and raise awareness for parents/carers and the community. Part of these sessions will provide parents with information on how the school protects children and young people whilst using on line technologies, such as the Internet. It will also be an opportunity to explore how the school is teaching children and young people to be safe and responsible Internet users and how this can be extended to use beyond the school environment.

The Appendices detail where parents/carers can go for further support beyond the school.

10. Links to other policies and documents

10.1 Cyber Bullying

Please refer to the Behaviour Policy and Anti-Bullying Policies for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. All behaviours should be seen and dealt with in exactly the same way, whether on or off-line and this needs to be a key message which sits within all ICT and PSHE materials for children and young people and their parents/carers. Children and Adults should not treat on-line behaviours differently to off-line behaviours and should have exactly the same expectations for appropriate behaviour.

10.2 Allegation against staff.
Please refer to the Guidance on dealing with allegations of abuse against teachers and other staff and the Whistle Blowing Policy in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Executive Headteacher immediately or Chair of Governors in the event of the allegation made about the Executive Headteacher.

Please refer to the Safeguarding Policy for the correct procedure in the event of a breach of child safety and inform the DSL within school immediately.

10.3 PSHE
We link the teaching and learning of e-Safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people. (See PSHE Policy)

10.4 School Website
The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always sought from the parent/carer prior to the uploading of any images. The school will consider which information is relevant to share with the general public on a website.

10.5 Social Media
All staff are trained on the use of social media during safeguarding and induction training. Staff should not make any contact with children via social media. Any inappropriate use should be reported to the Executive Headteacher.
Children are taught about appropriate use of social media during E-safety lessons.
Parents agree to appropriate use of Social media when signing the Home School Agreement.

Appendix 1

Staff Procedures Following Misuse by Staff

The Executive Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by an adult:

A. An inappropriate website is accessed inadvertently:

- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and LA/Easi PC so that it can be added to the banned or restricted list. Change Local Control filters to restrict locally.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down.
- Log the incident.
- Report to the Executive Headteacher and e-Safety Leader immediately.
- Executive Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the LA/Easi PC filtering services as with A.

C. An adult receives inappropriate material.

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Executive Headteacher immediately.
- Ensure the device is removed and log the nature of the material.
- Follow procedures detailed in the Safeguarding and Managing Allegations Policy.

D. An adult has used ICT equipment inappropriately:

- Follow the procedures for B.

E. An adult has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately, if necessary.
- Report to the Executive Headteacher and DSL immediately, who will follow procedures detailed in the Safeguarding and Managing Allegations Policy.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- Once Procedures and Policy have been followed and the incident is considered innocent, refer to the Acceptable Use Rules for Staff and Executive Headteacher to implement appropriate sanctions.

- If illegal or inappropriate misuse is known, contact the Executive Headteacher or Chair of Governors (if allegation is made against the Executive Headteacher) and DSL immediately and follow the Allegations procedure and Safeguarding Policy.
- Contact CEOP (police) as necessary.

F. Threatening or malicious comments are posted to the school website about an adult in school:

- Preserve any evidence.
- Inform the Executive Headteacher immediately and follow Safeguarding Policy as necessary.
- Contact the police or CEOP as necessary.

G. Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Executive Headteacher.

Appendix 2

Staff Procedures Following Misuse by Children and Young People

The Executive Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:

- Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
- Report website to the e-Safety Leader if this is deemed necessary.
- Contact the helpdesk filtering service for school and Easi PC so that it can be added to the banned list or use Local Control to alter within your setting.
- Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Decide on appropriate sanction.
- Notify the parent/carer.
- Inform Easi PC as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:

- Ensure the child is reassured and remove them from the situation immediately.
- Report to the Executive Headteacher and DSL immediately.
- Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
- If illegal or inappropriate misuse the Executive Headteacher must follow the Allegation Procedure and/or Safeguarding Policy.
- Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website about a child in school:

- Preserve any evidence.
- Inform the Executive Headteacher immediately.
- Inform Easi PC and e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:

- Preserve any evidence.
- Inform the Executive Headteacher immediately.

N.B. There are three incidences when you must report directly to the police via the Multi Agency Safeguarding Hub (See Safeguarding Policy).

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found. They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.
• www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Acceptable Use Rules for Staff

These rules apply to all on-line use and to anything that may be downloaded or printed.

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, these rules will be discussed regularly at staff meetings and as part of the induction procedures. This is so that they provide an example to children and young people for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I know that I should only use the school equipment in an appropriate manner and for professional uses.
- I understand that I need to give permission to children and young people before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's or young people's safety to the Executive Headteacher, Designated Person(s) for Child Protection or e-Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Person(s) for Child Protection are.
- I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should use the school E-mail and phones (if provided) and only to a child's school E-mail address upon agreed use within the school.
- I know that I should not be using the school system for personal use unless this has been agreed by the Executive Headteacher and/or e-Safety Leader.
- I know that I should complete virus checks on my laptop and encrypted memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the GDPR policy and have checked I know what this involves.
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.
- I have been given a copy of the E-safety Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

Signed …….. Date …….

Print name ……

E-Safety Acceptable Use Rules Letter to Parents/Carer

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet.
In order to support the school in educating your child/young person about e-Safety (safe use of the Internet), please read the following Rules with your child/young person then sign and return the slip.
In the event of a breach of the Rules by any child or young person, the E-Safety Policy lists further actions and consequences, should you wish to view it.
These Rules provide an opportunity for further conversations between you and your child/young person about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).
Should you wish to discuss the matter further please contact the Executive Headteacher.
Yours faithfully,
Xxxxxxx

E-Safety Acceptable Use Rules Return Slip, 200x – 200x

Child Agreement:
Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.

- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Key Stage 1

Our Internet and E-mail Rules

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We can send and open messages with an adult.
- We can write polite and friendly e-mails or messages to people that we know.
- We only tell people our first name.
- We learn to keep our password safely.
- We know who to ask for help.
- If we see something we do not like we will tell an adult immediately.
- We know that it is important to follow the rules.
- We will always log off the computer when we have finished using it.
- We will not tell people where we go to school or where we live.

Key Stage 2

Our rules for using the Internet safely and responsibly.

- We use the Internet to help us learn and we will learn how to use the Internet safely and responsibly.
- We send e-mails and messages that are polite and friendly.
- We will only e-mail or chat to people an adult has approved.
- Adults are aware when we go on-line and we know we are not allowed to do so without an adult in the room.
- We never give out passwords or personal information (like our surname, address or phone number).
- We never post photographs or video clips to approved websites and with an adult's permission.
- If we need help we know who to ask.
- If we see anything on the Internet or in an e-mail that makes us uncomfortable, we tell an adult immediately.
- If we receive a message sent by someone we don't know we do not open it until we have gained an adult's permission.
- We know we should follow the rules as part of the agreement with our parent/carer.
- We are able to look after each other by using our safe Internet in a responsible way.
- We know that we can go to www.thinkuknow.co.uk for help.
- We will always log off the computer when we have finished using it.

The Ashby Federation

Device loan agreement for pupils

1. This agreement is between:

1) The Ashby Federation ("Denton and Yardley Hastings Primary Schools") and Parent Name: …….

And governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to the school.

All issued equipment shall remain the sole property of the school and is governed by the school's policies.

- The school is lending the pupil a laptop ("the equipment") for the purpose of doing school work at home.
- This agreement sets the conditions for taking an Ashby Federation laptop home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times whether on the school's property or not.

If the equipment is damaged, lost or stolen, I will immediately inform Mrs Louise Brown, and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to the school in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure we take the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas
- We will not install/delete any apps or programs.
- We will not make any changes to the laptop settings and will connect to our own secured home internet.

3. Acceptable Use

I agree that my child will follow the schools Acceptable Use and Internet Safety Rules in line with our E Safety Policy.

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Return date

I will return the device in its original condition to the School Office when requested to do

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

6. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL'S NAME	
PARENT'S NAME	
PARENT'S SIGNATURE	
DATE	