Cleves Cross Primary School

Acceptable Use Policy

Policy Adopted: March 2018
Review Date: August 2019
Head Teacher: Mrs A Lazenby
Governor: Ms G Newby

A member of the Cleves Cross Learning Trust

Cleves Cross Primary School

Acceptable Use Policy

At Cleves Cross we believe it is important that the rights of our children are protected and fully supported by all members of staff. This policy takes into consideration these rights and in particular Article 13 (Freedom of expression): Children have the right to get and share information, as long as the information is not damaging to them or others. In exercising the right to freedom of expression, children have the responsibility to also respect the rights, freedoms and reputations of others. Also, according to Article 24 – children have the right to a safe environment. This includes online and by agreeing to and following an acceptable use policy, the children are keeping themselves and their peers safe.

Introduction

At Cleves Cross Primary School we understand that technology is an important tool for both teaching and learning. We also accept that as a school we hold personal data on learners, staff and other people to help us conduct our day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

Monitoring

Authorised IT staff may inspect any IT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any IT authorised staff member will be happy to comply with this request.

IT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

Through the use of the newly installed Smoothwall, the headteacher will also receive regular reports showing internet based searches and any items which have been deemed inappropriate. The headteacher can also access information regarding internet use of any member of staff using school owned devices.

All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school IT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, where appropriate, the HCC Disciplinary Procedure or Probationary Service Policy.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the school's SIRO or Online-Safety Co-coordinator (Ashley Robinson). Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to your Senior Information Risk Owner who is Alison Lazenby.

These will then be logged on the incident reporting form and will be dealt with following the school's related policies.

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

Password and Password Security

- Always use your own personal passwords
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures
- Staff should change temporary passwords at first logon
- Change passwords whenever there is any indication of possible system or password compromise

- Do not record passwords or encryption keys on paper or in an unprotected file
- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else.
- Ensure that all personal passwords that have been disclosed are changed once the requirement is finished
- Never tell a child or colleague your password
- If you aware of a breach of security with your password or account inform Ashley Robinson or Alison Lazenby immediately
- Passwords should contain a mixture of upper and lowercase letters, numbers and symbols
- User ID and passwords for staff and pupils who have left the school are removed from the system within 3 years (in accordance with County guidelines).

If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security

Personal or Sensitive Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment.
- Only download personal data from systems if expressly authorised to do so by your manager.

- You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

All documentation should be accessed through the Onedrive and no sensitive data should be removed from the school premises using removable media. If in the event this is not possible, staff should:

- Ensure removable media is purchased with encryption
- Store all removable media securely
- Securely dispose of removable media that may hold personal data
- Encrypt all files containing personal, sensitive, confidential or classified data
- Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password
- It is the responsibility of everyone to keep passwords secure
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared mopiers (multi-function print, fax, scan and copiers) are used.

Relevant Responsible Persons

Senior members of staff should be familiar with information risks and the school's response.

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

Information Asset Owner (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information and special educational needs data. A responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes
- what information needs to be protected how information will be amended or added to over time
- who has access to the data and why
- how information is retained and disposed of

As a result this manager is able to manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including DCC and network suppliers. Virus protection will be updated regularly. The school will comply with the terms of the data protection act, and is responsible for registering with the information commissioner's office . www.ico.gov.uk advice is available from www.ico.gov.uk/for_organisations/sector_guides/education.aspx

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission followed by an anti-virus / malware scan.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.

- The network manager will review system capacity regularly.
- The use of user logins and passwords to access the school network will be enforced.

How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home or personal information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or shared on the Learning Gateway. This is done through school photographic policy, and parents give permission for the child's school career.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- The school will scan regularly their own web site to check links that have been made into their own sites and to remove links from potentially dangerous sources.

How will pupil's images or work be published?

Still and moving images and sound add liveliness and interest to a publication, particularly when pupils can be included. Nevertheless the security of staff and pupils is paramount. Although common in newspapers, the publishing of pupils' names with their images is not acceptable. Published images could be reused, particularly if large images of individual pupils are shown.

Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. "Over the shoulder" can replace "passport style" photographs but still convey the educational activity. Personal photographs can be replaced with self-portraits or images of pupils' work or of a team activity. Pupils in photographs should, of course, be appropriately clothed.

Images of a pupil should not be published without the parent's or carer's written permission. Some schools ask permission to publish images of work or appropriate personal photographs on entry, some once a year, others at the time of use.

Pupils also need to be taught the reasons for caution in publishing personal information and images online.

- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or the parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.
- The School will have a policy regarding the use of photographic images of children which outlines policies and procedures

How will staff be consulted?

- All staff must accept the terms of the '**Responsible Internet Use**' and the **'Staff Code of Conduct'** statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet Policy, and Internet and E-mail Code of Practice and their importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the school Internet Policy will be provided as required.

Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such Smartphones, Blackberries, iPads, games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any members of the school community is not allowed.

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

Systems and Access

- You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own PC
- Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you
- Ensure you remove portable media from your computer when it is left unattended
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information
- Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period of time
- Do not introduce or propagate viruses
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act)
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act
- Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998
- It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever you appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

Staff and Pupil Involvement in Policy Creation

- Staff, governors and pupils have been involved in making/ reviewing the Policy for ICT Acceptable Use

Review Procedure

- There will be on-going opportunities for staff to discuss with the Online-Safety coordinator any Online-Safety issue that concerns them
- There will be on-going opportunities for staff to discuss with the SIRO/AIO any issue of data security that concerns them
- This policy will be reviewed every (12) months and consideration given to the implications for future whole school development planning
- The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way

Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

IT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Ashley Robinson (Online Safety coordinator) or Alison Lazenby.

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 policies 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 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) Mobile Phones

   a) Staff are responsible for their own mobile phones. These must be stored away during the school day and remain on silent. Mobile phones may only be used before/after school or during break times when children are not present.

   b) Staff mobile phones will never be used for any reason when children are present.

   c) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

   d) Staff mobile phones are allowed in school, but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming). Mobile phones should only be used for communication when not working with children and there are no children present.

   e) In the unlikely event of needing to contact a parent directly a school mobile phone will be issued to the member of staff concerned.

4) I understand that any device or hardware provided for by school is to be mainly used to complete official school. Use of any device for personal use, outside of school hours, is permitted, providing any actions/activities are lawful and in keeping with the ethos of the school.

5) Personal use of school ICT systems and connectivity is not permitted, only permitted with the consent of the head teacher, and only permitted outside of the school day, only permitted when children are not present.

6) 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.

7) 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).

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

9) Data Protection - *School should have a separate Data Protection Policy*

   a) I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. 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) or accessed remotely. Any personal 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. Secure means of transporting data are encrypted laptop / encrypted USB memory / encrypted HDD / approved cloud based system.

   b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

   c) I will not transfer sensitive personal information from my school e-mail account (e.g. Support Plans, Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

   d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones)

   e) Digital Images or videos of pupils will {Not be taken away from the school premises OR Only taken from the school premises using encrypted memory OR alternative secure transport method}

   f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

11) I will respect copyright and intellectual property rights.

12) Social Media

a) I have read and understood the school Online Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

b) I will not communicate with parents, pupils or ex-pupils under the age of 18 using any personal social media account. Any communication with parents must be completed through the official Cleves Cross Twitter account (see point e).

c) If any request is made by pupils or parents, staff should take a photo/screen shot and report this to Online Safety Coordinator (Ashley Robinson). Parents will then be informed and a discussion will take place with parents about the appropriate use of social media. This will then be logged in the online safety incident record.

d) My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via school twitter, a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team. *This would include any relatives of current pupils that are my “friends” on a social media site.*

e) My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

f) 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. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children’s online safety to the Designated Child Protection Coordinator (Alison Lazenby) and the Online Safety Coordinator (Ashley Robinson) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Ashley Robinson) the Online Safety Coordinator the designated lead for filtering as soon as possible.

14) 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 (Stuart Copeland) as soon as possible.

15) I will promote e-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.

16) 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 (Ashley Robinson) or the Head Teacher.

17) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……..……………………..………… Date ……………………

Full Name ………………………………..(printed)

Job title . . . .

Key Stage 1 Pupil e-safety agreement

Keeping me safe at home and at school

We only use the internet when a grown-up has said we can.

We tell a grown-up if something makes us feel worried or concerned.

If we get stuck or lost on the internet we will ask for help.

We will only write messages to people we know and these will always be friendly messages.

We will keep our personal information including: our name, address, school and pictures 'Top Secret' and not share these things on the internet.

We will not bring our mobile phones to school.

Pupil's E-safety Contract

Please complete and return to the child's class teacher

Pupil:	Class:
Pupil's Agreement: I have read and understood the pupil's e-safety contract and I will follow these rules to help keep myself and the rest of the school safe.	
Signed:	Date:
Parent's Consent I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety. I will ensure that any pictures taken during school events that include other children will not be shared using social media.	
Signed:	Date:
Please print name:	

Key Stage 2 Pupil e-safety agreement

Keeping me safe at home and at school

For my own personal safety – everywhere!

- I will only use the internet at school when I have been told I can
- I will never give out my personal information – passwords or logins
- I am aware of 'stranger danger' and will not try to meet people I meet online
- I will tell an adult if anything I see online makes me feel worried or uncomfortable
- I will never try to bypass the system and access content that has been blocked
- I understand that the school can monitor the websites I use and can check my files
- I will be careful when sharing pictures of myself or friends and if I am in school will always check with an adult first

Keeping the system safe

- I will only use my own login and passwords
- I will not attempt to access other people's files
- I will not use the school computers to play games, unless the teacher has given me permission
- I will not attempt to install software onto the school computers
- I will not use the system for gaming, gambling, shopping, or uploading videos or music

Responsibility to others

- Any messages I send will be polite and responsible
- I will not upload images or video of other people without their permission
- Where work is copyrighted (this included videos, pictures and music) I will not download or share with other people
- I understand that if I am involved in any incidents of inappropriate behaviour school can take action and the police may be informed if necessary

Personal Devices

- The school cannot accept responsibility for loss or damage to personal devices
- It is not permitted for children to bring mobile phones into school
- Other electronic devices (gaming consoles, iPads, tablets, cameras) should only be brought into school with permission from a teacher
- If a member of staff has any concerns then a mobile device can be checked to ensure the content is suitable. The child would be expected to unlock their device if asked

Pupil's E-safety Contract

Please complete and return to the child's class teacher

Pupil:	Class:

Pupil's Agreement:
I have read and understood the pupil's e-safety contract and I will follow these rules to help keep myself and the rest of the school safe.

Signed:	Date:

Parent's Consent
I have read and understood the e-safety agreement and give permission for my son / daughter to access the Internet at school, and will encourage them to abide by these rules. Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school. I understand that the school will take reasonable precautions to ensure pupils cannot access inappropriate materials. I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

I will ensure that any pictures taken during school events that include other children will not be shared using social media.

Signed:	Date:

Please print name: