Safe Use of ICT Policy

Aim

Information and Communication Technology (ICT) plays an enormously important part in the lives of all children and gives them unrivalled opportunities for information sharing and communication. It also brings risks. It is an important part of our role at Carrdus, and the aim of this policy, to teach our pupils how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks including identity theft, cyber-bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.

ICT in the curriculum

ICT is an important part of every academic subject at Carrdus. It is also taught as a subject, Computing. Our classrooms are equipped with Promethean ActivPanels smart boards and computers. We have a Computer Room with PCs and iPads; the use of computers, devices and the Internet is always supervised by an adult. All our pupils are taught how to research on the Internet and to evaluate sources. They are educated in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution - some sites that appear to be serious, impartial, historical sites, masquerade as sources of racist, homophobic, jihadist or other propaganda and some on-line encyclopaedias do not evaluate or screen the material posted on them. We teach our pupils about safe use of the internet and electronic safety (e safety) through our Computing and PSHE curricula. We will ask parents when their child/children start at Carrdus for permission to publish work on the Internet eg school website/social media.

Role of staff

With the explosion in technology, we recognise that blocking and barring sites is no longer adequate. We need to teach all our pupils to understand why they need to behave responsibly if they are to protect themselves. This aspect is a role for our Designated Safeguarding Lead (DSL), who has overall responsibility for the safeguarding of all our children including the EYFS and all our staff. Our technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our hardware system, our data and for training our teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the DSL. We ask all adults working in school to inform us that they have read, understood and agree to abide by Appendix 1: Agreement for the Safe Use of ICT for Adults Working in School.

Role of our Designated Safeguarding Lead

We recognise that internet safety is a child protection and general safeguarding issue. Our DSL, and Deputy DSLs, have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. They work closely with the Northants Safeguarding Children Partnership (NSCP) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of the school. All our staff, as part of their safeguarding training, have also received training in e-safety issues. It is the Head's responsibility to handle allegations of misuse of the internet.

Misuse of ICT and Filtering

We will not tolerate any illegal material and will always report illegal activity to the police and/or the NSCP. If we discover that a child is at risk because of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy, which includes guidance on cyber-bullying.
We have appropriate filtering in place and our children are always supervised whilst using the internet.

Involvement of Parents

We seek to work closely with parents in promoting a culture of e-safety. We will always contact parents if we have any worries about their son or daughter's behaviour in this area, and we hope that parents will feel able to share any worries with us. We recognise that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home. We therefore hold regular presentations for parents when an outside specialist advises about the potential hazards of this technology and the practical steps that parents can take to minimise the potential dangers to their sons and daughters without curbing their natural enthusiasm and curiosity. We ask pupils and/or their parents (dependent on age) to inform us that they have read, understood and agree to abide by either Appendix 2: Agreement for the Safe Use of ICT for Pupils in Nursery to Year 2 or Appendix 3: Agreement for the Safe Use of ICT for Pupils in Year 3 to Year 6; whichever is relevant.

Safe use of photographic and video images and personal information

While we recognise that publicity and pictures of children enjoying school is an essential part of school life, the aim of this policy is to ensure that no inappropriate photographs or recorded images of children are taken, that it is not possible to identify children from photographs accompanied by inappropriate information and that the inappropriate use/adaptation of images for use on child pornography websites cannot occur.
To ensure this we ask that the following rules, also found in our Safeguarding Policy, are observed:

- Ensure parents/carers have granted their consent for the taking and publication of photographic and video images;
- All children featured in photographs/recordings must be appropriately dressed for the activity with outer clothing garments covering their torso from at least the bottom of their neck to their thighs (i.e. a minimum of vest/shirt and skirt/shorts);

- Photography or video recording should focus on the activity rather than a child. Where possible, images of children should be recorded in small groups (the group may comprise any combination of adults and children);
- Staff must only use school cameras/devices to take pictures/recordings. School cameras/devices should not leave the site unless pass protected. If a school camera/device is lost it must be reported to the Head;
- Staff must not use their own personal devices for taking pictures/recordings. They should keep any personal devices away from children. They may only use their personal phones when not in contact with children. They should not contact families or children with their own phones.
- Personal details which might make a child vulnerable including name, address, email address and telephone numbers should not be revealed;
- Where possible, photographs/recordings should represent the diverse range of children participating in the activities;
- Anyone taking photographs or recording at any event, on behalf of the school, must have a valid reason for doing so and must have received permission from the School Office. They should make themselves known to the person in charge and be able to identify themselves if requested during the event;
- Staff working in our marketing department may use school or their own devices. They will fully delete all pictures/recordings once marketing work has been completed.
- All concerns regarding inappropriate or intrusive photography or video recordings should be reported in confidence to the Head;
- Teachers may use stand-alone/device-based video equipment as a learning aid and as a means of recording special occasions. However, care should be taken in the dissemination and storage of the material;
- To guard against the possibility of a child under a court order appearing on a website, the simultaneous streaming of images involving children onto a website/platform is not recommended. Delayed streaming also provides an opportunity for the editing of inappropriate clips (e.g. disarranged clothing);
- If parents or other visitors are intending to photograph or video at an event, they should be prepared to identify themselves, if requested, and state their purpose.
- We ask parents to video/photograph for their own use only and to not share photographs or videos on social media; we will remind parents before events.
- Pupils and parents should be informed that if they have concerns about inappropriate or intrusive photography/filming, these should be reported to the Head and recorded in the same manner as any other child protection concern. The Head might need to refer the issue to the local police force if this person continues to record images unauthorized;
- Staff should approach and challenge any person taking photographs/videos who has not made him/herself known;
- Staff have a whistleblowing responsibility to report other staff's misuse of mobile phones.

Review

This policy is monitored annually and is reviewed every 3 years by the DSL and DDSLs.

Appendix 1: Agreement for the Safe Use of ICT by Adults Working in School

Agreement

We will send out a Safe Use of ICT Agreement Form to all adults working in school. They will need to electronically return this agreement form to the school office.
Staff will be asked to agree to the following:

- I have read, understood and agree to follow our **Safe Use of ICT Policy;**
- I have read and understood the **e safety rules** for Lower and Upper School;
- I have read, understood and agree to abide by this **'Agreement for the Safe use of ICT by Adults working in School'**.

Use of Internet

All adults must:

- Not give anyone access to their login name or password;
- Not open other people's files without express permission;
- Not corrupt, interfere with or destroy any other user's information;
- Not release personal details including phone numbers or personal e-mail addresses of any colleague or pupil over the Internet;
- Not reproduce copyright materials without first getting permission from the owner. Many people will make their work freely available for education on request. Acknowledge sources on all resources used;
- Not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use;
- Not use school internet access for business, profit, advertising or political purposes – this is strictly forbidden;
- Always close browser and log out/shut down when a session has finished to enable others to log on/start up any computer on network;

Use of Phones

All adults must:

- Only use personal phones in school for personal use;
- Always use personal phones away from children and always store out of the reach of children;
- Always use a school camera/device for taking photos/videos.
- Only telephone parents, using a school mobile phone or the school landline phone, during school-working hours, unless in an emergency or on a day/residential trip.
- Ensure phone messages are positively supportive of children, staff and school and maintain the confidentiality of school information.

Use of Email and Messaging

All adults must:

- Follow school guidelines for the use of e-mail contained in the Safe Use of ICT Policy;
- Only use issued school email account/address to contact persons or organisations relating to work in school, including parents and other carers;
- Not use messaging services to communicate with parents including texting and WhatsApp. If they are themselves a parent with children at the school and are wishing to email or to use messaging services, they: must use a private email address or a private messaging service account.
- Must not use school year WhatsApp groups;
- Ensure emails and other messages are positively supportive of children, staff and school and maintain the confidentiality of school information;
- Send or respond to emails within 48 hours and between 7am and 8pm, except in an emergency;
- Understand that all emails are in the public domain and are not private; they may be monitored;
- Not include offensive or abusive language in messages or any language which could be considered defamatory, obscene, menacing or illegal;
- Ensure emails from school accounts are professionally and carefully written including tone, grammar, punctuation and spellings;
- Not use language that could be calculated to incite hatred against any ethnic, religious or other minority; be aware that school email may be monitored;
- Make sure nothing in the messages could be interpreted as libellous;
- Not send any message which is likely to cause annoyance, inconvenience or needless anxiety;
- Not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes;
- Inform Head if offensive, threatening or unsuitable email from within school or from external account is received.

Use of Social Media

All adults must:

- Only use devices provided by school to access and upload school related images or text to school social media accounts;
- Not post any school related images or text on their own personal social media accounts including personal social media accounts that are not in their own name but could be attributed to them;
- Not comment on any school related images or text on their own personal social media accounts;
- Not follow/accept Carrdus families on their own personal social media accounts including Facebook, Twitter and Instagram. If they are themselves a parent with children at the school and are wishing to follow/accept families, to do this through another family member; Ensure social media messages are positively supportive of children, staff and school and maintain the confidentiality of school information;
- Ensure parents/carers have granted their consent for the taking and publication of photographic and video images;
- Ensure children featured in photographs/recordings are appropriately dressed for the activity with outer clothing garments covering their torso from at least the bottom of their neck to their thighs;
- Ensure photography or video recordings focus on the activity rather than a child, unless child is being interviewed for marketing purposes;
- Ensure, where possible, images of children are recorded in small groups, not individuals, unless child is being interviewed for marketing purposes;

- Ensure personal details which might make a child vulnerable including name, address, email address and telephone numbers are not revealed;
- Ensure, where possible, photographs/recordings represent the diverse range of children participating in the activities.

Using of Internet with children

All adults must:

- Remind children of the rules for using the Internet and email (Appendix 3 and 6: e safety rules);
- Watch for accidental access to inappropriate materials and report the offending site to the DSL;
- Check before publishing children's work making sure parental permission has been sought;
- Ensure children cannot be identified from photographs;
- Report any breaches of the school's Internet policy to the DSL.

Appendix 2: Consent for the Safe Use of ICT by Pupils

Keeping children safe on the internet

As part of our updated 'Safe Use of ICT Policy', we think it is important that parents and carers are aware of the e safety rules we all abide by when using the internet in school. The children are taught how to stay safe when they begin to use the internet and further teaching takes place during Computing and PSHE lessons. Since the Internet is an essential and statutory part of our curriculum and a necessary tool for staff and pupils, we have a duty to provide pupils with quality internet access as part of their learning experience. For more information on how to keep children stay safe on the internet please take time to explore www.childnet.com

Consent

We will send out a Safe Use of ICT Consent Form to families. Parents and carers will need to return this consent form to the school office before their children are allowed to use ICT in school.
Parents and carers will be asked to consent to the following:

- I have read and understood the school's **e safety rules** and have discussed them with my child/children.
- I understand that although a teacher is always present and the school takes all reasonable precautions through firewalls and filters to ensure that pupils cannot access inappropriate materials, this risk cannot be eliminated.
- I therefore understand that the school cannot be held responsible for the content of materials accessed through the Internet.
- I agree that the school is not liable for any damages arising from inappropriate use of the Internet.

Appendix 3: e Safety Rules

e Safety Rules for Pupils in Lower School (Nursery to Year 2)

- These rules help us to stay safe on the Internet at Carrdus and at home.
- Do not share your school login and password with others.
- Always be sensible and careful when using technology that is connected to the internet.
- School tablets and computers should only be used with permission of a trusted adult.
- Always remember to sign out when you are finished on a school or shared computer.
- Keep your electronic devices safe and leave them at home.
- Remember: Think first then Click!
- Only click on buttons or links if you know what they do, or a trusted adult has told you it is safe to do so.
- Only use or search the Internet when a trusted adult is with you or has told you what to do.
- If you find or see something that upsets you, or you feel is wrong, stop and tell a trusted adult.
- Never tell anyone you do not know anything about yourself on the Internet, always check with a trusted adult first.

CARRDUS SCHOOL

e Safety Rules for Pupils in Upper School (Year 3 to Year 6)

- These rules help us to stay safe on the Internet at Carrdus and at home.
- Always be sensible and careful when using technology that is connected to the internet.
- Remember: Think first then click or ask on your device
- Treat all devices with respect no matter who they belong to.
- If a device is broken or not working properly inform a trusted adult so it can be repaired.
- Always remember to sign out when you are finished on a school or shared computer.
- Only use your own login name and password. Do not give this information to anyone.
- School tablets and computers should not be used to access gaming or social media sites.
- If you are using your own device at school, you should not be accessing gaming or social media sites.
- Remember you should never have content on your device that could upset others.
- A friend is someone you know, never accept an invite or add someone you do not know as a friend.
- Block anyone that upsets you and tell a trusted adult.
- Never give out your or another's address, phone number or arrange to meet someone over the Internet.
- If you see, find or are sent anything you are uncomfortable with, **stop** and tell a trusted adult.
- Keep the cameras on your devices covered when you bring them into school.
- You are not allowed to film in school unless directed so to do by a trusted adult and you do not want yourself filmed without your knowledge.
- Only use your school email for school related work and do not share it with others outside of school, unless you are told it is safe by a trusted adult.
- Only send e-mails that are polite and friendly.
- Never open an e-mail sent by someone you do not know.
- Never open an email attachment if you do not know it comes from a trusted source, ask a trusted adult if you are unsure.
- Forwarding of chain letter emails/messages or posts is not permitted in school.
- Remember many forms of social media are not appropriate for you to use until you are older. Age restrictions are there to **protect you** from harm.
- If you use social media at home, always send polite and friendly messages and remember parents or teachers may ask to see any messages we post.

- If you see a rude or offensive message or post from anyone at any time, whether in or out of school, **stop** capture an image and report it to a trusted adult. Always keep yourself safe
- Remember that the school may check your computer files and monitor the internet sites you visit.
- You must check with a trusted adult before accessing an unfamiliar website.
- Remember that some websites are a source of unreliable and inaccurate information. If you are unsure about information you have found, ask a trusted adult to check it with you.
- Keep your personal electronic devices including smart watches, cameras and gaming devices safe at home. Only bring a device to school if asked to by a teacher.
- Remember you are not allowed to take personal devices, (e.g. phones, cameras, trackers or smart watches) on any school trip, day or residential.