Kibworth CE Primary School

A place of discovery and friendship

E-Safety Core Policy

Written September 2007

Last Reviewed September 2018

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The previous Internet Policy has been extensively revised and renamed as the Kibworth C of E Primary School' e-Safety Policy to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Information Security.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from Schools Broadband including the effective management of Lightspeed filtering.
- National Education Network standards and specifications.

E-Safety Audit

This audit has been carried out by the senior leadership team (SLT) to assess whether the basics of e-safety are in place. Kibworth C of E Primary School will also design learning activities that are inherently safe and might include those detailed within Appendix 1.

The school has an e-Safety Policy that complies with CFE guidance.	Y
Date of latest update:	
The Policy was agreed by governors on: 01/02/2016	
The Policy is available for staff and for parents on the Website	
The Designated Child Protection Coordinator is **Gilly Paterson**	
The e-Safety Coordinator is **Nick Bradley**	
Do staff receive regular n e Safety training?	Y
All staff sign an Acceptable ICT Use Agreement on appointment.	Y
Parents sign and return an agreement that their child will comply with the school Acceptable ICT Use statement.	Y
Rules for Responsible Use have been set for students:	Y
These Rules are displayed in all rooms with computers.	Y
Internet access is provided by an approved educational Internet service provider and complies with DfES requirements for safe and secure access.	Y
The school filtering policy has been approved by SLT.	Y
An ICT security audit has been carried out by DSAT	Y
School personal data is collected, stored and used according to the principles of the GDPR.	Y
Staff with responsibility for managing filtering and network access monitoring work within a set of procedures and are supervised by DSAT ICT department	Y

2.2 Teaching and learning

2.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.3 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

2.2.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2.3 Managing Internet Access

2.3.1 Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.

2.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

2.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Publishing pupil's images and work

- 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 Website or Blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Twitter feed by way of signed Media Agreement.
- Pupil's work can only be published with the permission of the pupil and parents.

2.3.5 Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.6 Managing filtering

- The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing & Skype will be appropriately supervised for the pupils' age.
- Skype will be managed by the supervising adult who will connect using a protected password.
- Use of video for teaching purposes; i.e.; IRiS – agreement is sought from the parents where media agreements have not been signed or where the material will be made public.

2.3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

2.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

2.4 Policy Decisions

2.4.1 Authorising Internet access

- All staff, visitors, governors and trainees must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return the acceptable use policy.

2.4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The Discovery Schools Academy Trust cannot accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

2.4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher or reported using the whistle blowing procedures
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

2.4.4 Community use of the Internet

- The school will liaise with local organisations to establish a common approach to e-safety.

2.5 Communications Policy

2.5.1 Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.

2.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

2.5.3 Enlisting parents' support

- Parents' will be signposted to e-Safety resources in newsletters and on the school Web site.

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for Safeguarding.

- Our e-Safety Policy has been agreed by senior leadership team and approved by governors.
- The e-Safety Policy and its implementation will be reviewed annually.
- The e-Safety Policy was revised by: Michael Beck
- It was approved by the Governors on: 10/10/2018
- It will be reviewed: September 2109

Appendix 1

Kibworth C of E Primary School

e-Safety Rules

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

Pupil: ***(insert name)***	***Class:*** ***(insert class)***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Internet Access

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

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

Signed:	***Date:***

Please print name:

Please complete, sign and return to the school


Childnet International
www.childnet.com
Be Smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
THINK U KNOW
You can report online abuse to the police at www.thinkuknow.co.uk
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.

Staff ICT Acceptable Use Policy

1. Purpose 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 organisation's computer systems 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 organisations systems, they are asked to read and sign this ICT Acceptable Use Policy (AUP). This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the organisations ethos, GDPR regulations, other appropriate policies, relevant national and local guidance and expectations, and the Law.

2. Scope The policy applies to: • All DSAT employees. • Information assets, whatever format, device or medium they are held in. • All DSAT owned information, in whatever format, wherever it is held (e.g. by a third party) for which DSAT is the data controller.

3. Employee Responsibilities

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

ii. Discovery Schools Academy Trust Ltd 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.

iii. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff. 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.

iv. 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 6 or more characters and is changed regularly.

v. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from your line manager or the IT Department.

vi. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the General Data Protection Regulation (GDPR). This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site's (such email) will be encrypted by a method approved by the IT Department. Any images or videos of pupils will only be used in line with organisational policy and will always take into account parental consent.

vii. I will not keep professional documents which contain organisation-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones). If I choose to access the organisations email system on my mobile device (tablet or mobile phone), the device must be pin or password protected. I will protect the devices in my care from unapproved access or theft.

viii. Personal data kept on work devices must be kept to a minimum (examples that do not meet this include; Filling the hard drive with music files or photos).

ix. I will respect copyright and intellectual property rights.

Updated for GDPR – April 2018

x. I have read and understood the Social Media policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

xi. I have carried out Data Protection and GDPR training via the Flick online training portal.

xii. I have read and understood the DSAT Mobile Phone and Loaned Property Equipment policy that covers the use of any phone/loaned equipment that I may have been provided in order to carry out my work.

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

xiv. I will not attempt to bypass any filtering and/or security systems put in place by the organisation. If I suspect a computer or system has been damaged or affected by a virus or other malware, to the ICT Department as soon as possible.

xv. I will report any actual or potential data breaches to the Local Data Protection Representatives with 24 hours of the incident using the agreed Information Security Incident Form.

xvi. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via approved communication channels e.g. via a provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking.

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

xviii. 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 organisation I work for into disrepute.

xix. I will promote online safety and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

xx. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance. This includes the use of monitoring software on staff member's laptops.

xxi. I understand this forms part of the terms and conditions set out in my contract of employment.

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

Signed: ……

Print Name: ……

Date: ……