Christopher Reeves
Living Our Values

e-Safety Policy

February 2019

Christopher Reeves VA Primary School
Hinwick Road, Podington

1. Introduction and Overview

1.1 Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Christopher Reeves Primary School with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Christopher Reeves Primary School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils

1.2 The main areas of risk for our school community can be summarised as follows:

Content

- exposure to inappropriate content, including: online pornography, political or religious radicalisation, ignoring age ratings in games (exposure to violence associated with often racist language), and inappropriate websites, for example pro-anorexia/self-harm/suicide sites/hate sites)
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online, internet or gaming)
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.3 Scope

This policy applies to all members of Christopher Reeves Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school

The Education and Inspections Act 2006 empowers Head Teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that takes place out of school.

1.4 Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website/staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

1.5 Handling complaints:

- The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.
- Staff and pupils are given information about infringements in use and possible sanctions to include:
    - interview Headteacher;
    - informing parents or carers;
    - removal of Internet or computer access for a period, (which could ultimately prevent access to the curriculum)
    - referral to LA / Police
- The E-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy
- Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

1.6 Review and Monitoring

The school has an e-safety coordinator who is responsible for document ownership, review and updates.

The e-safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

2.1 Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - Smartie the Penguin guidelines for young children;
    - to use Hector (dolphin icon) to flood the screen;
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer,

teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas

- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign

- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons

2.2 Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the school's e-safety education programme
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school's Acceptable Use Policies.

2.3 Parent awareness and training

This school

- Provides advice, guidance and training for parents, including:
    - introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - information in school newsletters and on the school web site;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3 Safe Practice

3.1 Managing the Internet

- School provides pupils with supervised access to Internet resources through the school's internet connectivity
- School is provided with an educational filtering system through Partnership Education, and in line with Local Authority guidelines
- Staff preview recommended sites, online services, software and apps before use
- Parents are advised to re-check and monitor sites suggested for homework
- All users must observe software copyright – it is illegal to copy or distribute school software, or unauthorised software from other sources

3.2 Safe Use of Images

Digital images are very easy to capture, reproduce and publish, and are therefore open to misuse. It is not always appropriate to take and store images of any member of the school community and therefore:

- We gain written consent of parents for capture and use of digital images – permissions are reviewed annually
- Mobile phones are strictly prohibited from classrooms during school / after school club hours
- Visitors are required to leave their mobile phones at the school office
- Staff are not permitted to use personal digital equipment to record images of pupils, staff or volunteers on school trips
- Pupils and staff must have the permission of the Headteacher before any image can be uploaded for publication
- Images of children retained for assessment or marketing purposes will be stored on the schools secure server; staff should delete any images temporarily held on iPads or laptops once these have been transferred, and should not be stored on usb devices under any circumstances
- Images of children will be removed at the end of the academic year in which the child leaves the school, unless they have been used for purposes of promoting the school, when parental and pupil permission for continued use will be sought

3.3 Managing Email

- Staff and Governors are provided with a school email account for all school business, as appropriate. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed
- Staff and governors should use their school email for all professional communications
- It is the responsibility of each account holder to keep their password secure
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses
- Staff must inform the Headteacher if they receive an offensive email
- Pupils are introduced to email as part of the Computing Programme of Study and are monitored accordingly

3.4 Managing the School Website and Facebook Page

- Both the school website and Facebook page must adhere to safe practice and policy of digital images and data protection
- The school manages and monitors the publishing and editing rights of website content, and class teachers are responsible for ensuring the e-safety of content on their class pages
- Staff are advised to create a professional use profile for connecting to the school Facebook page (see also Staff Code of Conduct for guidelines on connecting with each other and parents using personal Facebook profiles)
- Staff, pupils and parents must use the Facebook 'Share' facility with extreme caution, and under no circumstances share content that could identify individual staff, pupils or volunteers

3.5 Asset disposal

Details of all school-owned hardware will be recorded in a hardware inventory.
Details of all school-owned software will be recorded in a software inventory.
All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The school will only use authorised companies who will supply a written guarantee that this will happen
Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Policy Review

This policy will be reviewed in full by the Governing Body on an annual basis.

The policy was last reviewed and agreed by the Committee of the Governing Body on

Signed: ..... Date: 6/2/19
Chair of Governors

APPENDIX 1

SUMMARY RESPONSIBILITIES

The members of the school community are responsible for ensuring e-safety in the following ways:

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-safety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-safety incident • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

Designated Safeguarding Lead
 	
(working in partnership with...)
	• To take day to day responsibility for e-safety issues and take a leading role in establishing and reviewing the school e-safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the school community
	• To ensure that e-safety education is embedded across the curriculum
	• To liaise with ICT technical staff
	• To communicate regularly with the designated e-safety Governor / Full Governing Body to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
	• To ensure that an e-safety incident log is kept up to date
	• To facilitate training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• To stay regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

E-Safety Coordinator	• To plan an annual programme of e safety learning • To work with Computing lead to ensure age-appropriate provision and progression through the school • Liaise with outside agencies to support e-Safety in the curriculum

Role	Key Responsibilities
Governors / E-safety Governor	• To ensure that the school follows all current e-safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/technician	• To report any e-safety related issues that arises, to the e-safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • To inform the LA of issues relating to the filtering applied • To keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • Ensure that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the school's e-security and technical procedures
Office Manager	• To ensure that all data held on pupils on the school management information system (SIMS) has appropriate access controls in place

Role	Key Responsibilities
Teachers	• To embed e-safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's e-safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-safety coordinator • To maintain an awareness of current e-safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (NB: at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology • To know and understand school policy on the use of mobile phones, digital cameras and hand held devices • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home

Role	Key Responsibilities
Parents/carers	• To support the school in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement • To consult with the school if they have any concerns about their children's use of technology
External groups	Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

APPENDIX 2

Acceptable Use Agreement – Staff

APPENDIX 3

Acceptable Use Agreement – Pupils