Le Cateau Community Primary School

Le Cateau School e-Safety Policy

Introduction

Internet technology helps pupils learn creatively and effectively. It encourages collaborative learning and the sharing of good practice amongst all school stakeholders. The e-safety policy encourages appropriate and safe conduct and behaviour during this process.

Aims

Our aims are to ensure that all pupils, including those with special educational needs:

- will use the internet and other digital technologies to support, extend and enhance their learning;
- will develop an understanding of the uses, importance and limitations of the internet and other digital technologies in the modern world including the need to avoid undesirable material;
- will develop a positive attitude to the internet and develop their ICT capability through both independent and collaborative working;
- will use existing, as well as up and coming, technologies safely.

e-Safety Policy Scope

The school e-safety policy and agreements apply to all pupils, staff, support staff, external contractors and members of the wider school community who use, have access to, or maintain school and school-related internet and computer systems internally and externally.

Policy review schedule

- This policy was approved by the governing body on: 2nd December 2015
- The e-safety policy will be monitored termly and reviewed annually.
- The next review date is January 2018.

Additionally, the policy will be reviewed promptly upon:

- Serious and/or frequent breaches of the acceptable internet use policy
- New guidance by Government/LA/safeguarding authorities
- Significant changes in technology as used by the school or pupils in the wider community
- E-safety incidents in the community or local schools which might impact on the school community.
- Advice from the police

Monitoring and Evaluation

The e-safety committee will monitor and evaluate the e-safety policy. This committee will comprise:

- E-safety co-ordinator: Joy Baggaley
- Head teacher and school leadership team: Ian Mottram, Kate Maxwell, Judith Tate, Mike Buckle, Lynzi Ewbank, Sophie Bell, Jackie Hardman
- ICT technical support and network manager John Hamer, Schools ICT
- External IT contractors: The Specialists (web developer)
- Governors: Beki Bulmer, Scott Keohane
- Pupils: Digital Leaders
- Child protection officer: Kate Maxwell

In the event of an e-safety incident, the following people will be informed within school: Joy Baggaley, (e-safety co-ordinator) Kate Maxwell, (child protection officer) Ian Mottram, (Headteacher)

The Child Protection Officer, Kate Maxwell will be able to differentiate which e-safety incidents are required to be reported to CEOP, local police, LADO, Social Care and parents/carers.

The school will draw up an e-safety calendar detailing training, meetings, reviews, evaluations, teaching and learning provision, parental involvement, wider community involvement and governor involvement over an academic year.

Staff, parent and pupil e-safety audits and pupil questionnaires will inform e-safety learning and staff training requirements. This will gauge the impact and effectiveness of the e-safety provision and determine future e-safety targets.

How does the school provide e-safety education?

- E-safety advice included in every Computing teaching unit.
- E-safety as part of PSHE curriculum including (but not limited to): how to deal with cyber-bullying; how to report cyber-bullying; the social effects of spending too much time online.
- E-safety as part of pastoral care including assemblies by local PCSOs and PCs and presentations by the school's Digital Leaders.
- E-safety events, e.g. Safer Internet Day and Anti-Bullying Week.
- The School website contains an e-safety section for pupils and parents.
- E-Safety tips are included in the regular newsletter

Data Protection

- There is a separate Data Protection policy.

E-mail

- Pupils and staff will only use approved e-mail accounts when using the school network.
- Pupils will tell a member of staff if they receive inappropriate e-mail communications.
- Pupils will only use e-mail for approved activities.

Internet Access and Online Portfolios

- Staff will read and sign the *NYCC Acceptable Use Policy – ICT and e-Technology* before using any school ICT resource.
- Parents and pupils will read and sign an Acceptable Use Policy
- Pupils will be taught to use the internet responsibly and to report any inappropriate content to a responsible adult.

Mobile Phones and other handheld technology

Pupils are only permitted to have mobile phones or other personal handheld technology in school with the permission of the Headteacher. When pupils are using mobile technology (their own or that provided by the school) they will be required to follow the school's Acceptable Use Policy (AUP). Such items can be confiscated by school staff if they have reason to think that

they are being used to compromise the wellbeing and safety of others. (*Education and Inspections Act 2006, Sections 90, 91 and 94)*

School Website, Facebook Page and Twitter Account

- There is a separate Social Media Policy for staff.
- All staff who edit or publish web-based content must read and adhere to this policy.

Systems Security

- ICT systems security will be regularly reviewed with support from Schools ICT.

Web Filtering

- The school will work with Schools ICT to ensure that appropriate filtering is in place. The school's filtering is provided by http://www.smoothwall.net/solutions/education/

- Pupils will report any inappropriate content accessed to an appropriate member of staff.

Whole-School Responsibilities for Internet Safety

Headteacher

- Responsible for e-safety issues within the school but may delegate the day-to-day responsibility to a Senior Leader such as the e-safety co-ordinator.
- Ensure that the e-safety co-ordinator is given appropriate time, support and authority to carry out their duties effectively.
- Ensure that developments at Local Authority level are communicated to the e-safety co-ordinator.
- Ensure that the Governing Body is informed of e-safety issues and policies.
- Ensure that appropriate funding is allocated to support e-safety activities throughout the school.

e-Safety co-ordinator

- Primary responsibility: establish and maintain a safe ICT learning environment (under the direction of Senior Management).
- Establish and maintain a school-wide e-safety programme.
- Respond to e-safety policy breaches in an appropriate and consistent manner in line with protocols set out in policies, and maintain an incident log.
- Report to the Senior Leadership Team to review the effectiveness and impact of the policy.
- Establish and maintain a staff professional development programme relating to e-Safety.
- Develop a parental awareness programme.
- Develop an understanding of relevant legislation and take responsibility for their professional development in this area.

Governing Body

- Appoint an e-Safety Governor who will ensure that e-safety is included as part of the regular review of child protection and health and safety policies.
- Support the Headteacher and/or designated e-safety co-ordinator in establishing and implementing policies, systems and procedures for ensuring a safe ICT learning environment.
- Ensure that appropriate funding is authorised for e-safety solutions, training and other activities as recommended by the Headteacher and/or designated e-safety co-ordinator (as part of the wider remit of the Governing Body with regards to school budgets).
- Promote e-safety to parents and provide updates on e-safety policies.

Network Manager/Technical Support Staff

- Provide a technical infrastructure to support e-safety practices.
- Ensure that appropriate processes and procedures are in place for responding to the discovery of illegal materials, or suspicion that such materials are, on the school's network.

- Ensure that appropriate processes and procedures are in place for responding to the discovery of inappropriate but legal materials on the school's network.
- Develop an understanding of relevant legislation.
- Report network breaches of acceptable use of ICT facilities to the Headteacher and/or the e-safety co-ordinator.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Teaching and Support Staff

- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Include e-safety lessons as part of the Digital Literacy curriculum and use a cross curricular approach to the delivery of e-Safety guidance.
- Deal with e-Safety issues they become aware of and know when and how to escalate incidents.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Wider School Community

- This group includes: non-teaching staff; volunteers; student teachers; other adults using school network, internet, or other technologies.
- Contribute to the development of e-safety policies.
- Adhere to acceptable use policies.
- Take responsibility for the security of data.
- Develop an awareness of e-safety issues, and how they relate to pupils in their care.
- Model good practice in using new and emerging technologies.
- Know when and how to escalate e-safety issues.
- Maintain a professional level of conduct in their personal use of technology, both within and outside school.
- Take responsibility for their professional development in this area.

Parents and Carers

- Contribute to the development of e-safety policies.
- Read acceptable use policies and encourage their children to adhere to them.
- Adhere to acceptable use policies when using the school network.
- Discuss e-safety issues with their children, support the school in its e-safety approaches and reinforce appropriate behaviours at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Model appropriate uses of new and emerging technologies.
- Liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online.

Policy adopted by Governing Body and implemented: December 2015
Review: Annually
Last Review: January 2017
Next Review: January 2018
Lead member: Alice Thomas