Ridgeway Primary School

E-safety Policy

Policy written:	August 2017
Date of approval by Governors:	Sept. 2018
Date of Review:	Sept. 2019
Current Subject Leader:	Iain Wilson

Achieving our potential together.

Contents

1. Introduction and overview
- Rationale and Scope
- Roles and responsibilities
- How the policy be communicated to staff/pupils/community
- Handling complaints
- Review and Monitoring

2. Education and Curriculum
- Pupil e-safety Curriculum
- Staff and governor training
- Parent awareness and training

3. Expected Conduct and Incident management

4. Managing the ICT infrastructure
- Internet access, security (virus protection) and filtering
- Network management (user access, backup, curriculum and admin)
- Passwords policy
- E-mail
- School website
- Learning platform
- Social networking
- Video Conferencing

5. Data security
- Management Information System access
- Data transfer

6. Equipment and Digital Content
- Personal mobile phones and devices
- Digital images and video
- Asset disposal

Appendices:

1. Acceptable Use Agreement (Staff)
2. Acceptable Use Agreement (Pupils)
3. Acceptable Use Agreement including photo/video permission (Parents)
4. Protocol for responding to e-safety incidents
5. Protocol for Data Security
6. Search and Confiscation guidance from DfE

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Ridgeway Primary School with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Ridgeway 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 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 cyber bullying 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 students.

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

Content

- Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse.
- Lifestyle 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).

Scope

This policy applies to all members of Ridgeway 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 Ridgeway Primary School.

The Education and Inspections Act 2006 empowers Headteachers 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 academy, 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 take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for e-Safety provision. • To take overall responsibility for data and data security (SIRO). • 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.
E-Safety Co-ordinator / Designated Child Protection Lead	• Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents. • Promotes an awareness and commitment to e-safeguarding throughout the school community. • Ensures that e-safety education is embedded across the curriculum. • Liaises with school technical staff. • To communicate regularly with Governors 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. • Facilitates training and advice for all staff. • Liaises with the Local Authority and relevant agencies. • Is 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
Governors / Computing and 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 Curriculum Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Computing/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
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum. • To liaise with the e-safety coordinator regularly.

Role	Key Responsibilities
Network Manager/technician	• To report any e-Safety related issues that arises, to the Computing/e-Safety coordinator. • 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 Computing system. • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices. • The school's policy on web filtering is applied and updated on a regular basis. • 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. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place.
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. • 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 Policy. • I am aware that my usage of the internet will be monitored and disciplinary action may be taken for non-compliance. • 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. • 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.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy (at KS1 it would be expected that parents / carers would sign on behalf of the pupils). • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • 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. • To help the school in the creation/ review of e-safety policies
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.

Communication:

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

- Policy to be posted on the school website.
- 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.

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. Sanctions available include:

- interview with Computing/ e-Safety Coordinator / Headteacher;
- informing parents or carers;
- removal of Internet or computer access for a period,
- referral to LA / Police.

Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyber bullying 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.

Review and Monitoring

The e-safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an e-safety coordinator who will be 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.
- The e-safety policy has been written by the school Computing/e-safety Coordinator and is current and appropriate for its intended audience and purpose.

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

2. Education and Curriculum

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 SWGfL e-Safeguarding and e-literacy framewok for EYFS to Y6 and national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- 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;
- [for older pupils] to understand why and how some people will ‘groom’ young people for sexual reasons;
- to understand the impact of cyber bullying, 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 cyber bullying; 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.

We plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas, and we will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network. Our staff will model safe and responsible behaviour in their own use of technology during lessons and ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights.
We will ensure that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

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 program.
- Provides, as part of the induction process, all new staff with information and guidance on the eSafeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school:

- Runs a rolling programme of advice, guidance and training for parents on internet safety awareness.
- Holds training events for parents to raise the profile of e-safety.

3. Expected Conduct and Incident management

Expected conduct

In school all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (at KS1 it would be expected that parents/carers would sign on behalf of the pupils.);
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should 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;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.

Staff

- Are responsible for reading the school's e-safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

Pupils

- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies, as part of the e-safety acceptable use agreement form at time of their child's entry to the school.
- Should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

Incident Management

In school:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (eg the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with e-safety issues;
- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in e-safety within the school;
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.