Online Safety Policy
Ridgeway Primary School
June 2019

CONTENT **PAGE**

1. Introduction:

1.1 Purpose of policy

The purpose of this policy is to ensure that staff and pupils have a clear understanding of their responsibilities and school procedures with regard to Online Safety.

It is not intended that pupils study this document and the key points appertaining to their role and responsibility are posted in summary form at key locations around the school.

2. Roles and Responsibilities:

Online Safety Governor: Mr Chris Ecob.
Online Safety Co-ordinator: Miss Laura Gray
Designated Teacher for Safeguarding: Miss Laura Gray (Deputy Headteacher)
Deputy Designated Teacher: Mrs Joanne Jelves (Headteacher)
Deputy Designated Teacher: Mrs Deb Derry (Learning Mentor)
Deputy Designated Teacher: Mrs Gemma Middleton (Deputy Headteacher)
Deputy Designated Teacher: Mrs beth Sedgley (Educare Co-ordinator)
Deputy Designated Teacher: Miss Laura Wem (Senior Educarer)
Safeguarding Governor: Mrs Pam Potter
Technical Support: Mr Rob Jelves.

The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school:

2.1 Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. A member of the Governing Body has taken on the role of Online Safety Governor

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors committee / meeting

2.2 Headteacher and SLT:

The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community,

The Headteacher / Senior Leaders are responsible for ensuring that the Online Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their Online Safety roles and to train other colleagues, as relevant

- The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff. See Annex A

2.3 Online Safety Co-ordinator:

- takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the school Online Safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.
- provides training and advice for staff on at least an annual basis
- liaises with school ICT technical staff
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- reports regularly to Senior Leadership Team

2.4 Technical Support:

Mr Rob Jelves will ensure:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments.
- that the school meets the Online Safety technical requirements outlined in the Staffordshire Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that they keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- that monitoring software / systems are implemented and updated as agreed in school policies.
- Incidents of misuse are reported to the Online safety co-ordinator and relevant members of SLT in order to inform future Online safety developments.
- that they carry out regular audits and reviews of the safety and security of the school ICT systems.

2.5 Teaching and support staff:

Are responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (AUP) See Annex B
- they report any suspected misuse or problem to the Online Safety Co-ordinator for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems

- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school Online Safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

2.6 Designated Child Protection Teacher:

Should be trained in Online Safety issues 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

(NB: It is important to emphasise that these are child protection issues, not technical issues, it is simply that the technology provides additional means for child protection issues to develop)

3. E-Force

- A pupil voice group devoted to matters of Online Safety (The E-Force) will meet fortnightly during pupil voice meetings to discuss ways to improve Online Safety around school.

- Assemblies will be prepared and delivered by the E-Force annually to children of Key Stage 1 to keep them updated with Online Safety matters and to collect their pupil voice.

4. Pupils:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy (Annex C), which they will be expected to sign before being given access to school systems. The appropriate Pupil AUP will be issued on entry to the school and again in Year 3 as pupils move from Key Stage 1 to Key Stage 2. In EYFS and at KS1 it would be expected that parents / carers would sign on behalf of the pupils, having discussed the policy with their children first. Children joining school at other times in the school year will be issued with the policy and associated documents upon entry to the school.
- 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 Online Safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

5. Parents/Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.

Parents and carers will be responsible for discussing and endorsing (by signature) the Pupil Acceptable Use Policy.

6. Visitors and Community users:

Community Users who access school ICT systems / website as part of the Extended School provision will be expected to read then sign a Visitor AUP (Annex D), before being provided with access to school systems. Other visitors to school will be shown the agreed usage policy and will be expected to sign the Visitor AUP. They will be issued with a temporary visitor's log on.

7. Policy statement:

7.1 Curriculum

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages in the use of ICT across the curriculum**.**

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Online Safety Co-ordinator can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. The ICT Technician will re-block the site immediately following the lesson.
- pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

7.2 Agreed Usage:

The school will try to ensure that pupils will have good access to ICT to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

8. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or,

very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity ie.
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The flow chart from the Staffordshire Safeguarding Children's board– Annex A and http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/_should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.

NB: In such cases DO NOT print out any evidence, save it and report it.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the contact the Staffordshire Safeguarding Children's Board.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible and in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as detailed in the Behaviour and Anti Bullying and Safeguarding policies.

9. Use of Social Network sites such as Facebook

- The school blocks access to all social networking sites.
- It is inappropriate for pupils to ask or have school staff as 'friends' on social networking sites.
- It is inappropriate for school staff, to accept school pupils, past and present, as 'friends' on social networking sites, such as Facebook.
- School policy is that staff will remain professional when accessing or interacting with Social Networking sites out of school hours.
- Staff will ensure that the privacy levels on their own social network accounts are as such that they cannot be accessed by pupils or parents of the school ensuring that their privacy is maintained.
- Incidents where Facebook is found to be being used by pupils to post comments which are abusive, threatening or hurtful towards other pupils or adults in school or where comments damage the reputation of the school, sanctions will be applied in line with the School Behaviour Policy and could in some circumstances result in exclusion.

This policy should not be seen as the school condoning the use of sites such as Facebook outside of school and neither are we encouraging the use of it. The purpose of this section of the policy is to raise parents awareness of the risks of underage use of such sites, so that Parents can make informed decisions as to whether to allow their child to have a profile or not.

Should parents decide to allow their child to have a social media profile we strongly advise that they:

- Check that their child's profile is set to private and that only friends can see information that is posted.
- Monitor their child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos.
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a bookmark on their profile to CEOP and the Report Abuse button which has been known to deter offenders.
- Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Set up your own profile so you understand how the site works and ask them to have you as a 'friend' on their profile so you know what they are posting online.
- Make sure your child understands the following rules:
    - **Always keep your profile private**
    - **Never accept friends you don't know in real life**
    - **Never post anything which could reveal your identity**
    - **Never post anything you wouldn't want your parents to see**
    - **Never agree to meet somebody you only know online without telling a trusted adult**
    - **Tell someone if you feel threatened or someone upsets you**

We would recommend that all parents visit the CEOP Think U Know website for more information on keeping your child safe online www.thinkuknow.co.uk

Any incident where Facebook, or other mobile technology are being used to post abusive, threatening or hurtful comments about another member of the school community (pupils or adults), which is reported to the school by a parent or member of the public will be dealt with, and sanctions issued, in line with the school's behavior policy, including in some circumstances the possibility of exclusion.

10. Staff Training and CPD:

10.1 Education –pupils

The education of pupils in Online Safety is an essential part of the school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of ICT / PHSE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. Online Safety lessons will take place at least termly.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies each term.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Rules for use of ICT systems / internet will be posted in all relevant areas.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

- Internet Safety Day will be celebrated across the school, to raise awareness.

10.2 Education – parents / carers
The school will seek to provide information and awareness to parents and carers through letters, newsletters and the web site.

10.3 Education - Extended Schools
The school will offer family learning courses in ICT, media literacy and Online Safety so that parents and children can together gain a better understanding of these issues. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

10.4 Education & Training – Staff
It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal Online Safety training will be made available to staff.
- All new staff should receive Online Safety instruction as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies
- The Online Safety Coordinator will receive regular updates through attendance at LA training sessions and by reviewing guidance documents released by BECTA / LA and others.

10.5 Training – Governors
Governors should take part in Online Safety training / awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents

11. Infrastructure.

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their Online Safety responsibilities.

The Online Safety coordinator will ensure that outside service providers are aware of the Staffordshire Security policies and AUP.

School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in the LA Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance

- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted

Areas of access to information are restricted for pupils and staff as determined by the Head teacher

All users from KS1 upwards will be provided with a username and password by the ICT co-ordinator who will keep an up to date record of usernames.
Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

12. Use of digital and video images - Photographic, Video

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a 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 (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix)
- Videos or photographs taken by parents etc at school events /such as concerts) shall be for private use only and may not be shared, published or distributed. A statement to this effect will be made prior to any such event.

13. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (all staff have been issued with a memory staff containing a password protected partition)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school Data Protection Policy once it has been transferred or its use is complete

14. Legislation.

All Staff and Governors should be aware of the relevant legislation which is incorporated into the framework of this policy. These are listed in Annex E.

15. SMSC Statement

At Ridgeway Primary School we recognise that SMSC development is central to the education of all pupils and therefore it is taught and reflected in all areas of the curriculum and through all aspects of school life.

16. Prevent Statement & British Values

At Ridgeway Primary School we aim to prepare our students to become good citizens of the future. Through our curriculum we teach pupils British Values and how to celebrate diversity. We aim to raise their awareness of radicalisation and extremist views, whatever the source. We have adopted the principles and advice found in 'Keeping Children Safe in Education 2015' and the 2011 'Prevent Strategy'. These are incorporated into our school policy on tackling extremism.

17. Related Policies:

Safeguarding
Child Protection
Anti Bullying
Behaviour
Data Protection Policy (Please refer to school office)

Miss Laura Gray
Deputy Headteacher
June 2019

Document History

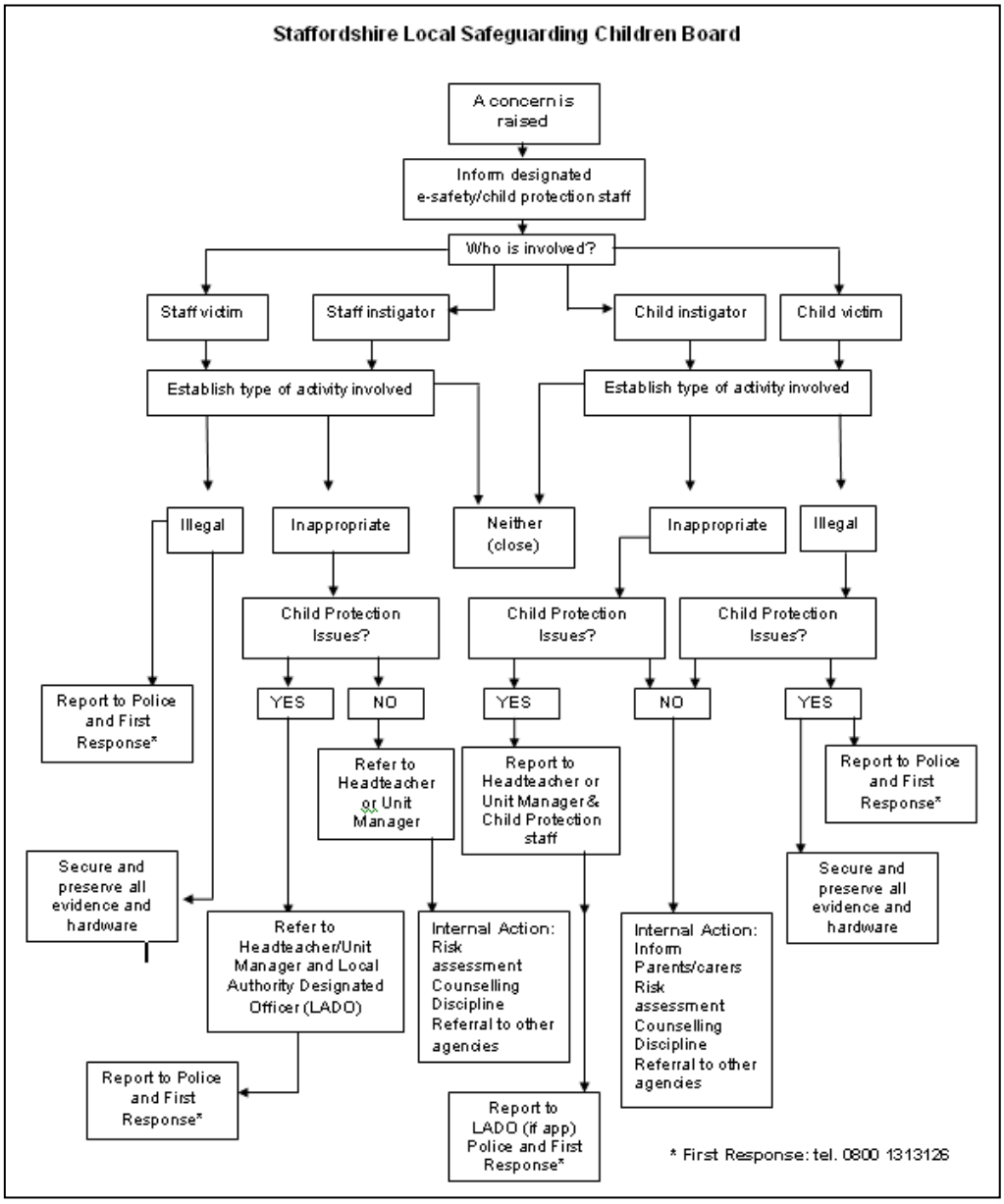
June 2011	Adopted at Governing Body meeting 28th June 2011
January 2013	Updated to include section on social networking presented to Personnel Committee 24th January 2013
September 2014	Change of names for persons responsible for safeguarding in school

February 2017	Full review presented to Pupil Well Being Committee 6th March 2017 for adoption
June 2019	Presented for re adoption at Pastoral Committee 11th June 2019 with minor changes to staffing.

This policy is due for review 2020

Annex A. Responses to Incidents

The flowchart from the Staffordshire Safeguarding Children's board– below and http://www.staffsscb.org.uk/e-SafetyToolkit/IncidentResponse/ should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



Annex B. Staff "Acceptable Use policy"

Ridgeway Primary School

Acceptable Usage Policy – Staff

Rules for E-Mail and Internet Use.
February 2017

1 Introduction

1.1 Schools are using E-mail and the Internet more and more to support their activities. This E-mail and Internet use policy, which will form part of our ICT Security Policy, contains the rules for using the E-mail and Internet facilities. It applies to all school staff who use either or both of these facilities.

1.2 As well as saying what you are not allowed to use E-mail and the Internet for, the policy also provides guidance on the good practices that you should use and the practices that you should avoid.

1.3 The school will periodically review the policy in response to guidance issued by the County Council.

2 Access to E-mail and Internet services

2.1 Your connection to E-mail or the Internet must be authorised (in writing or in electronic form) by your System Manager. All school Internet access will be via an approved Internet Service Provider (ISP). Any variations to this must be authorised in writing by the Headteacher.

2.2 You must choose the ISP's filtering option if one is available.

2.3 The school E-mail and Internet facilities are for business use but we will allow staff to use them privately, as long as it is reasonable. If you use these facilities, you must keep to and not break any of the conditions in this policy.

2.4 The school has the right to monitor E-mails and Internet use.

2.4 If you intentionally access a computer system or information without permission, you are breaking the law under the Computer Misuse Act 1990.

3 Code of Conduct Declaration

3.1 If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration / consent form to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy.

3.2 The school will keep the signed declaration in you're the school office. We will ask you to confirm that you still understand and accept the rules annually.

4 Specific Conditions of Use

4.1 General prohibitions

4.1.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use the E-mail and Internet facilities for reasons that are:

- pornographic or obscene;
- intimidating, discriminatory (for example; racist, sexist or homophobic) or that break our anti-harassment and equal opportunities policies in any other way;
- defamatory;
- encouraging violence or strong feelings;
- hateful;
- fraudulent;
- showing or encouraging violence or criminal acts;
- unethical or may give us a bad name; or
- a deliberate harmful attack on systems we use, own or run.

4.1.2 We will only allow you to do the above if:

- it is part of your job to investigate illegal or unethical activities;
- your Headteacher or System Manager asks you to in writing; or
- it is in the public interest.

You must make sure that your System Manager knows what you are doing. If you find or suspect anyone of using the computer system illegally or unethically, you must report it to your System Manager who will advise your Headteacher or Chair of Governors or Internal Audit.

4.1.3 You must not use the school E-mail or Internet facilities for time-wasting activities, such as chain letters, or for sending private E-mails to everyone on the global address list.

4.2 Computer viruses

4.2.1 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:

- intentionally accessing or transmitting computer viruses or other damaging software; or
- intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

4.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet and train you in its use. You must not E-mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and tell your System Manager.

4.2.3 You must always follow the instructions that your System Manager gives you about virus attacks.

4.2.4 If you are not sure how to use the virus protection system, you must get advice from your System Manager.

4.3 Passwords

4.3.1 You must not tell anyone your password, apart from authorised staff.

4.4 Other security

4.4.1 You must not use or try to use the school facilities for:

- accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- breaking through security controls on any system; or
- accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

4.5 Publishing information

4.5.1 You must get authorisation from the Headteacher for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site We will not allow the publishing or editing of Web sites which involve advertising, financial reward or are part of a business.

4.6 Copyright

4.6.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through E-mail or over the Internet.

4.6.2 You must not:

- transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
- knowingly download or transmit any protected information that was written by another person or organisation without getting permission from the owner.

4.7 Confidential or sensitive information

4.7.1 You must not break the conditions of the Data Protection Act 1998 when you use the E-mail services of the Internet for transmitting information.

4.7.2 The Internet E-mail facility is not a secure way of transmitting confidential, sensitive or legally privileged information unless there are special security measures (such as encryption). Without these security measures, Internet E-mail is as insecure as a postcard that you send through the normal post. So, you should make sure that the Internet is suitable for transmitting information that you feel is confidential, sensitive or legally privileged. If you allow anyone to see this type of information without permission, you may be breaking the law.

4.7.3 If you have to transmit any E-mail over the Internet that you think contains confidential, sensitive or legally privileged information, no matter what special security measures you take, you are strongly advised to include the following disclaimer in the E-mail.
'This E-mail (including any attachments) is only for the person it is addressed to. If you are not this person, you must delete this E-mail immediately. If you allow anyone to see, copy or distribute the E-mail, or if you do, or don't do something because you have read the E-mail, you may be breaking the law'. This disclaimer can be set using the 'autosignature' facility where this is available.

4.8 Recording Internet use

4.8.1 You should be aware that use of ISP facilities is logged.

4.8.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to your System Manager or Headteacher. If you do not do this, the school may take action against you.

4.8.3. You should protect yourself by not allowing unauthorised people to use your Internet facility.

5 E-mail good practice

5.1 The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use internal or Internet E-mail services at Ridgeway Primary School.

5.2 **You should:**

- check your E-mail inbox for new messages regularly;
- treat E-mail as you would a letter, remember they can be forwarded / copied to others;
- check the message and think how the person may react to it before you send it;
- make sure you use correct and up to date E-mail addresses;
- file mail when you have dealt with it and delete any items that you do not need to keep;
- All emails pertaining to school related issues must be sent through a school email address (@ridgeway.staffs.sch.uk). Personal email addresses may not be used for school purposes.

5.3 **You should not**:

- use E-mail to manage staff where face-to-face discussion is more appropriate;
- create wide-distribution E-mails (for example, to addressees throughout the world) unless this form of communication is vital;
- print out messages you receive unless you need a hard copy;
- send large file attachments to E-mails to many addressees;
- send an E-mail that the person who receives it may think is a waste of resources;
- use jargon, abbreviations or symbols if the person who receives the E-mail may not understand them.

Ridgeway Primary School - ICT Agreed Usage Policy

Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in the school office.

Declaration:

I confirm that, as an authorised user of the School's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Acceptable Usage Policy for Staff including 'E-mail & Internet Use - Good Practice'.

Your details:
Name:

Job title:

Signature:

Date:

The above named policies may be found in the Staff Handbook or are available by request from the Computing Co-ordinator. They are also downloadable from www.ridgeway.staffs.sch.uk in PDF format.

Please return your completed form to the school office.
Thank you

Annex C. Acceptable Usage Policy – Pupils (EYFS & Key Stage 1)

Ridgeway Primary School

Rules for using the internet, e-mail and the computers at Ridgeway.

EYFS and KS 1.

We use the school computers and Internet for learning, school work and homework. These rules will help us to be fair to others and keep everyone safe.

I will ask my teacher before I go onto the internet

I will use only my own login and I will keep it a secret.

I will not look at, change or delete other people's files.

I will not put anything into the computer (eg: disks) without asking an adult.

I will only e-mail people I know, or my teacher has asked me to.

The messages I send will be polite and sensible.

I will ask an adult before opening an e-mail or an e-mail attachment.

If I see anything I am unhappy with or I receive messages I do not like, I will tell an adult immediately.

I know that the school may check my computer files and may monitor the Internet sites I visit.

I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Annex C. Acceptable Usage Policy – Pupils (Key Stage 2)

Ridgeway Primary School

Rules for using the internet, e-mail and the computers at Ridgeway.

We use the school computers and Internet for learning, school work and homework. These rules will help us to be fair to others and keep everyone safe.

I will ask permission before entering any Web site, unless my teacher has already said it's OK.

I will use only my own login and password, which I will keep secret.

I will not look at, change or delete other people's files.

I will not bring storage media (e.g. USB devices, R/W CDROMS, etc) to use in school without permission.

I will only e-mail people I know, or my teacher has approved.

The messages I send will be polite and sensible.

When sending e-mail, I will not give my home address or phone number, or arrange to meet someone.

I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.

I will not use Internet chat or post material on you-tube about myself or my classmates.

If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.

I know that the school may check my computer files and may monitor the Internet sites I visit.

I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Ridgeway Primary School

Rules for using the internet, e-mail and the computers at Ridgeway: Pupil & Carer Agreement.

Please complete, sign and return to the school office.

All policies relating to Online Safety are available to view at www.ridgeway.staffs.sch.uk or from the school office.

Pupil's name:	***Class:***

Pupil's Agreement:

I have read, or my parent/carer has read to me, and I understand the school 'Rules for using the internet, e-mail and the computers at Ridgeway' document. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed:	***Date:***

Parent / Carer's Consent for Internet Access:

I have read and understood the school document 'Rules for using the internet, e-mail and the computers at Ridgeway' and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or 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:

Parent / Carer's Consent for Web Publication of Work and Photographs:

I agree that, if selected, my child's work may be published on the school Web site. I also agree that photographs that include my child may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed:	***Date:***

Annex D. Acceptable Usage Policy – Visitors.

Ridgeway Primary school

Acceptable Usage Policy – Visitors

Rules for E-Mail and Internet Use.

February 2017

Code of Conduct Declaration

1.1 If you use or have access to our E-mail or Internet facilities, you need to read this policy carefully and make sure that you understand it. The school will provide appropriate training. You then need to sign the declaration/consent form to confirm that you have read, understood and will keep to the policy. You must also understand that we may take action against you if you wilfully break the conditions of the policy.

1.2 The school will keep the signed declaration on record. Sometimes, we may ask you to confirm that you still understand and accept the rules.

Specific Conditions of Use

2.1 **General prohibitions**

2.1.1 You must not use, or try to use, our E-mail and Internet facilities to create, distribute or display in any form, any activity that is or may be considered to be against the law or against our rules and policies. In this context, you are not allowed to use E-mail and Internet facilities for reasons that are:

- Pornographic or obscene;
- Intimidating, discriminatory (for example; racist, sexist, homophobic) or that break our anti-harassment and equal opportunities policies in any other way;
- Defamatory;
- Encouraging violence or strong feelings;
- Hateful;
- Fraudulent;
- Showing or encouraging violence or criminal acts;
- Unethical or may give us a bad name; or
- A deliberate harmful attack on systems we use, own or run.

Computer viruses

2.2.1 It is a crime to deliberately introduce a computer virus, under the Computer Misuse Act 1990. You must not use the school E-mail and Internet facilities for:

- Intentionally accessing or transmitting computer viruses or other damaging software; or
- Intentionally accessing or transmitting information about, or software designed for, creating computer viruses.

2.2.2 You must scan any material you receive or download from the Internet to make sure it is virus free. The school will ensure that virus protection exists on any standalone or locally networked computers that can access the Internet. You must not E-mail material that has not been scanned to other users. If you find a virus, or you think the material has one, you must immediately break the connection, stop using the computer and report this to the school office.

Other security

2.3.1 You must not use or try to use the school facilities for:

- Accessing or transmitting information about, or software designed for, breaking through security controls on any system;
- Breaking through security controls on any system; or
- Accessing, without permission, any E-mail that is not for you, even if it is not protected by security controls.

Publishing information

2.4.1 You must get authorisation from the Head teacher for any school information that is to be published on the Internet. All schools have web space available for authoring of their own school web site. Images of individuals must have their permission or that of their parent/guardian before publication of the web site. We will not allow the publishing or editing or Web sites which involve advertising, financial reward or are part of a business.

Copyright

2.5.1 It is illegal to break copyright protection. You could break copyright if you download or transmit protected material through-mail or over the Internet..

2.5.2 You must not:

- Transmit copyright software from your computer to the Internet or allow any other person to access it on their computer through the Internet; or
- Knowingly download or transmit any protected information that was written by another person or organisation without getting permission form the owner. *Permission can be sought via e-mail.*

Recording Internet use

2.6.1 You should be aware that use of ISP facilities is logged.

2.6.2 If you access a prohibited Internet site unintentionally, you must break the connection immediately and report it to the school office. If you do not do this, the school may take action against you.

2.6.3 You should protect yourself by not allowing unauthorised people to use your Internet facility. When leaving your computer unattended for any length of time, the computer should be locked by using the ‘Control-Alt-Delete’ keys.

Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach ff ICT security to the school office or, in exceptional cases, the Head teacher.

You must be aware that any infringement of the current legislation relating to the use of ICT systems:-

Data Protection Acts 1984 & 1998
Computer Misuse Act 1990
Copyright, Designs and Patents Act 1988
The Telecommunications Act 1984

Provisions of legislation may result in disciplinary, civil and/or criminal action.

February 2017. MP.

Ridgeway Primary School - ICT Agreed Usage Policy

Visitor Declaration

You must read, understand and sign this form if you are undertaking any activity on the site of Ridgeway Primary School.

We will keep the signed declaration on file.

Declaration

I confirm that, as a visitor to Ridgeway Primary School, I have read, understood and accepted all of the Rules for ICT users in the Acceptable Usage Policy for Visitors.

Date	Name (please print)	Job title/reason for visit	Signature

February 2017. MP.

Annex E. Legislation

Schools should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

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