**Eldwick Primary School**

# E- Safeguarding Policy

| | |
|---|---|
| **Date Approved** | 13/1/14 |
| **Revised** | Feb 2015, Feb 2016, November 2017, November 2018 |
| **Author / Owner** | Mr P Cross |
| **Next Review date** | November 2019 |

## Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and adults are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school e-safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement; however, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies eg behaviour/bullying policies

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build both pupils' and adults' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

**The Scope of this policy**

This policy applies to all members of the school community including governors, staff, 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 students / 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 online bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

The policy has been developed and amended in response to GDPR (May 2018) with relevant sections checked against eSecurity requirements. Relevant sections have also been cross checked with the school's other policies to ensure comprehensive GDPR compliance.

**Roles and Responsibilities**

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

**Governors**

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Curriculum and Pastoral 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*

The role of the E-Safety Governor will include:

- *regular meetings with the E-Safety Officer*
- *regular monitoring of e-safety incident logs*
- *reporting to relevant Curriculum and Pastoral committee / meeting*

**Headteacher and Senior Leaders**

- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the *E-Safety Officer*.
- *The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant*
- *The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer.*
- 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 e-safety allegation being made against a member of staff.

**E Safety Officer**

- Leads the e-safety committee
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting of the Curriculum and Pastoral Sub Committee
- reports regularly to Senior Leadership Team

**School Technician**

The ICT Technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- ensures school meets required cyber security and eSafeguarding technical requirements;
- ensures users may only access the networks and devices through a properly enforced password protection policy; in which passwords are regularly changed.
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

**Teaching and Support Staff**

Teaching and support staff should ensure that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Officer for investigation / action / sanction
- digital communications with pupils (email / Virtual Learning Environment (VLE) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor ICT activity in lessons, extra curricular and extended school activities
- they are 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
- they use IT and school IT equipment appropriately both in and out of school
- in lessons where internet use is pre-planned students / 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
- In lessons where pupils will be searching for images staff should specify the words to search for and the sites to use. These should be checked as close to the actual lesson time as possible. If pupils wish to search for additional words staff should have a laptop turned away from the children and check the search for inappropriate material before allowing children to search

**Designated Person for Child Protection**

The Designated Leads are aware of e-safety issues and 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
- Online bullying

**E Safety Committee**

Members of the *E-safety committee* (Mr P.Cross, Mrs R.Sharp, Mrs J.Rosano, Mr A Dean) will assist the *E-Safety Coordinator / Officer (or other relevant person, as above)* with:

- the production / review / monitoring of the school e-safety policy / documents.
- *the production / review / monitoring of the school filtering policy (if the school chooses to have one)*
- Mapping and reviewing the eSafeguarding curricular provision – ensuring relevance, breadth and progression;

**Pupils**

- are responsible for using the school ICT systems in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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.

**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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through *parents' evenings, e safety text of the month, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.* Parents and carers will be encouraged to support the school in promoting good eSafeguarding practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

The school has made links with the local police community support officers who specialise in cybercrime, and arrange information evenings.

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

**Education**

**Pupils**

A planned e-safety programme is 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

- Key e-safety messages are reinforced as part of a planned programme of assemblies and pastoral activities
- During Safer Internet Day (SID) in February of each year, the opportunity is taken to reinforce key messages
- pupils are 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
- A planned Online Safety programme is delivered through ICT and PSHE in the form of the TIC Bradford scheme
- Rules for acceptable use are shared at the beginning of each academic year and with any new starters as they join school
- Pupils are taught how to search for information safely and safe search engines are used by Teaching Staff

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet
- Pupils are made aware of the process to follow if they see anything online which they find upsetting or which is unsuitable for children
- Pupils know that any events of online bullying are taken seriously by the school and they understand the importance of sharing their concerns with a trusted adult

**Staff**

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- The annual questionnaire results from Parents and Pupils will highlight issues relevant to the school and particular year groups. These will be used to direct training.
- Planning and online safety work will be monitored regularly and will be used to direct training.
- All staff will receive a briefing and a copy of the Acceptable use policy annually.
- Staff will receive a copy of the Online Safeguarding policy annually.
- Both policies are included in the induction pack for new starters.

**Governors**

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways; Governors service, online, 4LC collaborative INSET and school INSET.

**The use of digital images and 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 eg on social networking sites.

- *Staff are encouraged to take digital/video images to support educational aims with school owned devices. Use of personal devices is not permitted. When a cohort of children leaves school, digital images of them will be deleted along with their user accounts. A limited archive of special events containing images of children will be kept, for which specific permission is sought from parents on the parent consent form.*
- *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*
- *Pupils' full names will not be used anywhere on the website or blog, particularly in association with photographs.*

- *Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (may be covered as part of the AUP signed by parents or carers at the start of the year* .
- *Pupil's work can only be published with the permission of the student / pupil and parents or carers.*

- *Parents are told at all events that although we allow them to take photos and video they are not allowed to post them on any social media site. Any breech of this will result in us not allowing any photos or videos to be taken at events. Staff would ensure that any child who can't have their photograph taken will not appear in any photographs. If there is a risk to any child then photos will not be allowed. At the school disco, children are not allowed to bring their own phones and must hand them in when they arrive.*

**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.
- Access data only when logged on to the school network.

**Passwords**

All users (staff and pupils) have the responsibility for the security of their username and password and must not allow other users to access the systems using their log on details (as per Acceptable Use Policies). Any concerns about sharing passwords or log on details must be reported.

- Passwords for new users and replacement passwords for existing users can be allocated by the school technician.
- Members of staff are made aware of the school's password rules through induction, the Acceptable Use Policy and the Online Safeguarding policy.
- All pupils have their own individual log on and password for accessing the school's ICT systems.
- Pupils are made aware of the school's password rules through ICT/Online Safety lessons and through the Pupil Acceptable Use Policy.
- Old usernames and accounts are deleted annually.
- Pupils have individual passwords for logging into the network.

- Pupil passwords are set as follows:
  - Reception children have CVC words
  - Children in Year 1 and 2 have simple words and numbers
  - Children in Year 3 and 4 have a mixture of words and numbers
  - Children in Year 5 and 6 have a mixture of letters, numbers
- Staff passwords are set as follows:
  - They must be a minimum length of 8 characters
  - Users cannot use a password that has been used the last 2 times
  - Password change prompts will be the first week of every term
  - Passwords must meet complexity requirements
  - After 5 failed attempts. The user will be locked out for 15 minutes.

**Online bullying**

Cross reference with school behaviour policy

Online bullying is the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Examples of electronic communication are social networking web sites and apps, texting, use of other mobile or tablet apps, email or online software.

All members of the school community are reminded of the key messages in relation to e safety:

- Pupils and adults who feel as if they are being bullied in any way need to talk to someone who they trust. Pupils need to talk to a trusted adult.
- Make sure you keep any evidence of online bullying by taking screen captures. Make a note about the time and date of any of these messages and any details about the sender.
- Do not forward messages to other people, this means you are joining in the bullying. Stop it by reporting it to a trusted adult.
- Do not reply to any bullying messages, this could make things worse and shows the bully that they are getting a response from you.

The school may report serious online bullying incidents to the Police.

**Appropriate use by staff or adults**

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources.

They have a password to access a filtered service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.
All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Rules will be displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff in their 'Staff Files'.

Staff training will underpin the receipt of this policy.

When accessing school web sites from home, the same Acceptable Use Rules will apply. The acceptable use will be the same for both staff and children so that an example of good practice is established.

**In the event of inappropriate use**
If a member of staff is believed to misuse technological devices, the Internet or Learning Platform in an inappropriate, abusive or illegal manner, a report must be made to the Headteacher immediately. The Allegations Procedure and the Child Protection Policy will be followed to deal with any misconduct and all appropriate authorities contacted. Staff should be mindful of their professional status and teacher standards, as well as their standing in the local community, when using social networking sites.
In the lesser event of misuse or accidental misuse, appropriate action will be taken by the Headteacher.

**Appropriate use by children**
Acceptable Use Rules, will be signed and returned to school to keep under file along with a letter for children and parents/carers explaining how children are expected to use the Internet and other technologies within school or other settings. The rules are there for children to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

*The rules will be on display within the classrooms and in the computer suite.*

We want our parents/carers to support our rules with their child, by signing the Acceptable Use Rules together so that it is clear to the school, the rules are accepted by the child with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children may be using the Internet beyond school.

Further to this, we hope that parents/carers will add to future amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used at that time and reflect any potential issues that parents/carers feel should be addressed, as appropriate.

*The school council are actively involved in discussing the acceptable use of on-line technologies and the rules for misusing them.*

**In the event of inappropriate use**

Should a child or young person be found to misuse the on-line facilities whilst at school or in a setting the following consequences will occur (these will be reviewed by SLT, our school council and stakeholders as the policy is updated):

- Appropriate action (by a member of the SLT) will take place if any child is found to be misusing the Internet by not following the Acceptable Use Rules. This action may be:
  Discussion with child
  Request for discussion with parents
  Letter home
  Child not allowed to access technology for a period of time
  Additional education and training

In the event that a child or young person **accidentally** accesses inappropriate materials the child will report this to an adult immediately and take appropriate action to hide the screen or close the window, so that an adult can take the appropriate action.

Where a child feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice.

Children should be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

**Mobile devices**

**Staff**

During teaching time, while on playground duty and during meetings, mobile phones will be switched off or put on 'silent' mode. Staff must not use mobile phones in lessons. Except in urgent or exceptional situations, mobile phone use is not permitted during teaching time or while on playground duty. In accordance with the Acceptable Use Policy staff should not use personal devices for photography in school. Only School cameras or devices are to be used.

**Pupils**
School does not allow children to bring mobile phones into class. All mobile phones must be handed in to the office at the start of the day and are returned at the end of school.

As part of the Bradford E Safeguarding strand of the Computing Scheme of work pupils are taught about the dangers of using mobile phones, the fact that location services can say exactly where you are and how quickly children can post content online before thinking about the consequences.

**School's Mobile Devices**
The school has 32 iPads for use in class. The use of these devices is covered in the pupil and staff acceptable use policies. Pupils know that they must not take pictures of other people without their permission. They are not allowed to download or install apps on any device. These devices are subject to the same levels of internet filtering as all the school computers accessed by children. Automatic camera upload should be turned off to stop any photos taken from automatically uploading to Google Drive.

**Monitoring and Reviewing of the E Safeguarding Policy**

| | |
|---|---|
| This e-safety policy was approved by the *Curriculum and Pastoral Governors Sub Committee on:* | *14.1.13 and since on 14.01.14, February 2015, February 2016* |
| The implementation of this e-safety policy will be monitored by the: | *Mrs R Sharp E Safety Officer*<br>*Mrs R Sharp Named Child Protection Person*<br>*Mr Andrew Dean E Safety Governor*<br>*Mr P Cross ICT Coordinator*<br>*Mr M Day ICT Technician*<br>*Mrs J Rosano CEOP Ambassador* |
| Monitoring will take place at regular intervals: | *Annually* |
| The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals: | *Annually* |
| The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be: | *November 2019* |
| Should serious e-safety incidents take place, the following external persons / agencies should be informed: | *Jenni Whitehead*<br>*Bradford Council's Child Protection Development Co-ordinator* |

**Monitoring of the policy will take place through these actions**

- Recording incidents in an e safety log (see appendix)
- Weekly Smoothwall Records of breaches in authority wide lists of sites (from the Bradford Learning Network – telephone 01274 385844
- Carrying out e Safety behaviour surveys: www.ticbradford.com

# Acceptable Use Rules for Staff and Governors

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign these Acceptable Use Rules. This is so that they provide an example to children for the safe and responsible use of on-line technologies which will educate, inform and protect and so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

- I will only use the school equipment in an appropriate manner and for professional uses.
- I will only use my school email appropriately for school work/communication.
- I understand that I need to give permission to children before they can upload images (video or photographs) to the Internet or send them via E-mail.
- I know and ensure that that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.
- I have read the Procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.
- I will report accidental misuse.
- I will report any incidents of concern for children's safety to the Headteacher, Designated Person for Child Protection or e- Safety Leader in accordance with procedures listed in the Acceptable Use Policy.
- I know who my Designated Persons for Child Protection are.
- I will not make contact with or accept a current pupil of Eldwick on any social networking account I have. I know that I am putting myself at risk of misinterpretation and allegation should I contact children via personal technologies, including my personal e-mail. I will use the school E-mail and phones and only communicate appropriately through a child's school E-mail address whilst in class.
- I will not be using my school email for personal use.
- I will complete virus checks on my laptop and memory stick or other devices so that I do not inadvertently transfer viruses, especially where I have downloaded resources.
- I will only install hardware and software I have been given permission for.
- I will ensure that I follow the Data Protection Act 1998 and have checked I know what this involves. (See E safeguarding policy section on data protection)
- I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will inform the e-Safety Leader.
- I have been given a copy of the Acceptable Use Policy to refer to about all e-safety issues and procedures that I should follow.
- I will adhere to copyright and intellectual property rights.

I have read, understood and will adhere to the E safety Policy (January 2016) and the AUP Rules as I know that by following them I have a better understanding of e-Safety and my responsibilities to safeguard children and young people when using on-line technologies.

Signed……. Date……..

Name (printed)……

Eldwick Primary School
e-Safety Acceptable Use Rules Letter to Parents/Carer

Dear Parent/Carer,

At Eldwick Primary School we recognise the use of ICT and communications facilities as an important resource for teaching and learning. However, at times users will encounter risks, posed more by behaviours and values online than the technology itself. Consequently, during ICT and PSHCE lessons as your child accesses the Internet, E-mail and Learning Platform we will ensure they are taught and made aware of appropriate safe and responsible online behaviours to protect themselves and get the most out of the technology itself.

In order to support the school in educating your child about e-Safety (safe use of the Internet), please read the following Rules with your child then sign and return the slip.

In the event of a breach of the Rules by any child, the e-Safety Policy (located in the school policy file in the main entrance) lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact myself or the e-safety leader, Mrs R. Sharp.

Yours sincerely,

Mrs J.Kershaw
Headteacher

---

e-Safety Acceptable Use Rules Return Slip, 2015 – 2016

Child Agreement:

Name: _____Class:_____

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____ Date: _____

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: _____ Date: _____

Key Stage 1

These are our rules for using the Internet safely.

**Our Internet Rules**

- We use the Internet safely to help us learn.
- We learn how to use the Internet.
- We only tell people our first name.
- We learn to keep our password a secret.
- We will ask an adult if we need help.
- If we see something we do not like we will tell the teacher or our parent/carer.
- We know that it is important to follow the rules.
- We are able to look after each other by using our Internet safely.

Key Stage 2

These are our rules for using the e-safety and responsibly.

| Our E-Safety Rules |
| --- |
| • We use technology to help us learn and we will learn how to use it safely and responsibly.<br>• We ask permission from a member of staff before using a device.<br>• We send messages that are polite and friendly.<br>• We only use our school email address in school during lessons, with permission from a member of staff.<br>• We only e-mail people an adult has approved.<br>• Adults are aware when we use on-line tools.<br>• We will not use the usernames or passwords of others.<br>• We do not access other people's files.<br>• We never give out or share passwords or personal information (like our surname, address or phone number).<br>• We do not bring in data storage devices from outside school unless we have permission from a teacher.<br>• We never post photographs or video clips without permission and never include surnames with photographs.<br>• If we see anything that makes us uncomfortable, we will immediately hide the display (do not turn it off) and inform a teacher or parent/carer.<br>• If we receive a message sent by someone we don't know we know we will not reply and alert the teacher or parent/carer immediately.<br>• We do not bring mobile phones into school. |

**Useful Websites**

**www.thinkuknow.co.uk/teachers**
**www.childnet.com**
**www.kidsmart.org.uk**
**www.ceop.gov.uk/reportabuse/index.asp**