Inspiring each other to achieve success

Congerstone Primary School

Congerstone Primary School

Online Safety Policy

Adopted from: **School Policy based on** *Keeping Children Safe in Education (2014)policy provided at Online safety training course (summer2017*

Policy to be reviewed: annually

Last reviewed: **October 2018**

Date of next review: **October 2019**

Signed: …….. Date: ……
Chair of Governors

Name:

Signed: …….. Date: ……
Headteacher

Table of contents

Policy Statement

For clarity, the Online Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors..

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents

Safeguarding is a serious matter; at Congerstone Primary School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as Online Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the Congerstone Primary School website; upon review all members of staff will sign as read and understood both the Online Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Students Acceptable Use Policy will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
    - Report to the Safeguarding committee

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within our school. The day-to-day management of this will be delegated to the Online Safety Officer - Jodie Armstrong

The Headteacher will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Officer

The day-to-day duty of Online Safety Officer is devolved to *Jodie Armstrong Computing Co-ordinator*
The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all Online Safety matters.
- Engage with parents and the school community on Online Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.

- Retain responsibility for the Online Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support.
- Make him/herself aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any Online Safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Online Safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Staff will be encouraged to use passwords which are not easily guessed.
    - The IT System Administrator password is to be changed when required.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any Online Safety incident is reported to the Online Safety Officer (and an Online Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the Online Safety Officer or the Headteacher to make a decision.
- The reporting flowcharts contained within this Online Safety policy are fully understood.

All Students

The boundaries for use of Computing equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

Online Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; therefore school will ensure parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents evenings, school newsletters, text messages and emails school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such, parents will sign the student Acceptable Use Policy before any access can be granted to school equipment or services.

Online Safety Committee

Online Safety will be part of the remit for the Pupil Outcomes Governor Committee where they are responsible;

- to advise on changes to the Online Safety policy.
- to establish the effectiveness (or not) of Online Safety training and awareness in the school.
- to recommend further initiatives for Online Safety training and awareness at the school.

Technology

Congerstone Primary School uses a range of devices including PC's, laptops, iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use NetSweeper software that prevents unauthorised access to illegal websites. It also helps to prevent access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, Online Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Office365 for Education software helps prevent infected email being sent or received by school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the school on an un-encrypted device. Any breach (i.e. loss/theft of device such as laptop or USB keydrives) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office. *(Note: Encryption does not mean password protected.)*

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff passwords will change if there has been a suspected or confirmed compromise. Student passwords will be unique and age appropriate. Student passwords will be centrally managed and changed by a staff member if there is a suspected or confirmed compromise. The ICT Coordinator and IT Support will be responsible for ensuring that passwords are changed.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives (if you allow them) are to be scanned for viruses before use or on-access by school systems.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this Online Safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy. AUPs for all users will be renewed annually and managed by the School Business Manager.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly, use of personal email addresses for work purposes is not permitted.
Students are permitted to use the school email system, and as such will be given their own email address, when required.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic/Use of children's images Policy, and is re-iterated here for clarity. All parents must

sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Congerstone Primary School is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. The following social media services are permitted for use within Congerstone Primary School and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the Online Safety Officer who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

Twitter – used by Congerstone school as a broadcast service (A broadcast service is a one-way communication method in order to share school information with the wider school community. as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any Online Safety incident is to be brought to the immediate attention of the Online Safety Officer, or in his/her absence the Headteacher. The Online Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Congerstone Primary School will have an annual programme of training which is suitable to the audience.

Online Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning. There are also discrete lessons and sessions planned throughout the year based on the Rising Stars Switched On to Computing.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

The Online Safety Training Programme can be found on the Staff Area of the school network.

Acceptable Use Policy – Staff

Congerstone Primary School
Staff and Governor
Acceptable Use Agreement / Code of Conduct

- ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Headteacher and Online Safety Officer.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to pupils.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that any data (under the Data Protection Act) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Headteacher or Online Safety Officer
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies may be monitored and logged and may be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights. Including software licensing
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

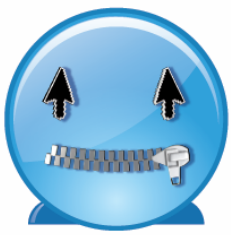
User Signature
I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..(printed)

Congerstone Primary School
Pupil Acceptable Use of the Internet
Agreement / eSafety Rules

- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own details such as my name, phone number or home address.
- ✓ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ✓ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

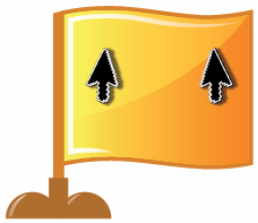


ZIP IT

Keep your personal stuff private and think about what you say and do online.

BLOCK IT

Block people who send nasty messages and don't open unknown links and attachments.



FLAG IT

Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

Letter to Parents to Accompany Online Safety Policy:

Dear Parents / Carers

Acknowledgement of Internet Use

As part of the ICT/computing Curriculum, your child will be taught how to use the Internet to search for information and how to send and receive email. You will be aware of the great increase in Internet use over the past few years and Congerstone Primary School believes that it is essential to teach the skills needed to access the Internet in order to equip children for life outside school.
We have taken a number of steps to ensure that access to the Internet is safe for your child whilst in school. The children will access the Internet through an Internet Service Provider. We use the LA recommended provider, which is especially designed for schools and filters out any undesirable material. Children will only have access to the Internet as part of planned lessons and when an adult is supervising. There are rules that children must follow and the school will not be liable for any damages arising from your child's use of the Internet.
The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school; in order to ensure that there have been no attempts of inappropriate Internet activity we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances. We may also use software to monitor screen activity both online and offline and will use this information to help us meet our safeguarding requirements. The Internet is a very powerful tool, which can be used to support your child's education. We ask that you fill in the attached slip, acknowledging your child's use of the Internet and return it to school.

If you have any questions or concerns, please do not hesitate to discuss them with your child's class teacher.

Alison Ruff
Headteacher

I am aware that my child will use the internet, email in school, under supervision, and understand the rules, which will govern that use.

Child's name:…… Class:……

Signed:…… Date:……..
Parent/Carer

Online Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, Online Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Risk Log(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	Online Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

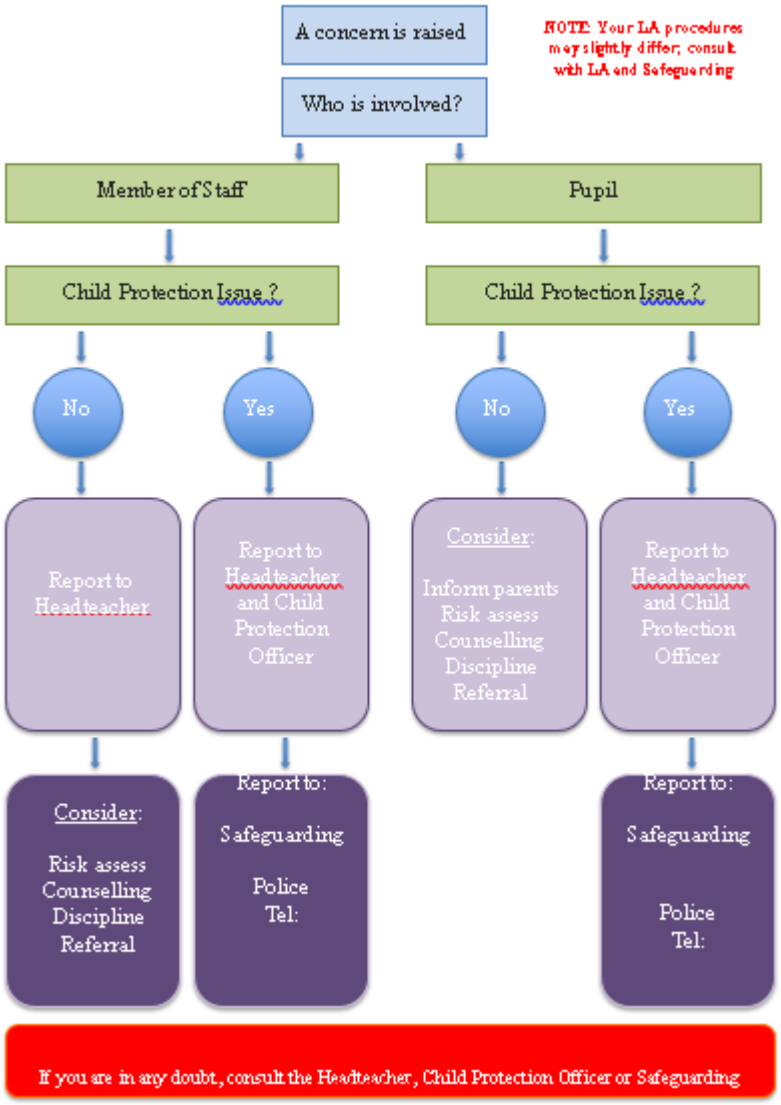
Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)
Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk **4 – 6 = Medium Risk** **7 – 9 = High Risk**

Owner: **The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.**
Final decision rests with Headteacher and Governing Body

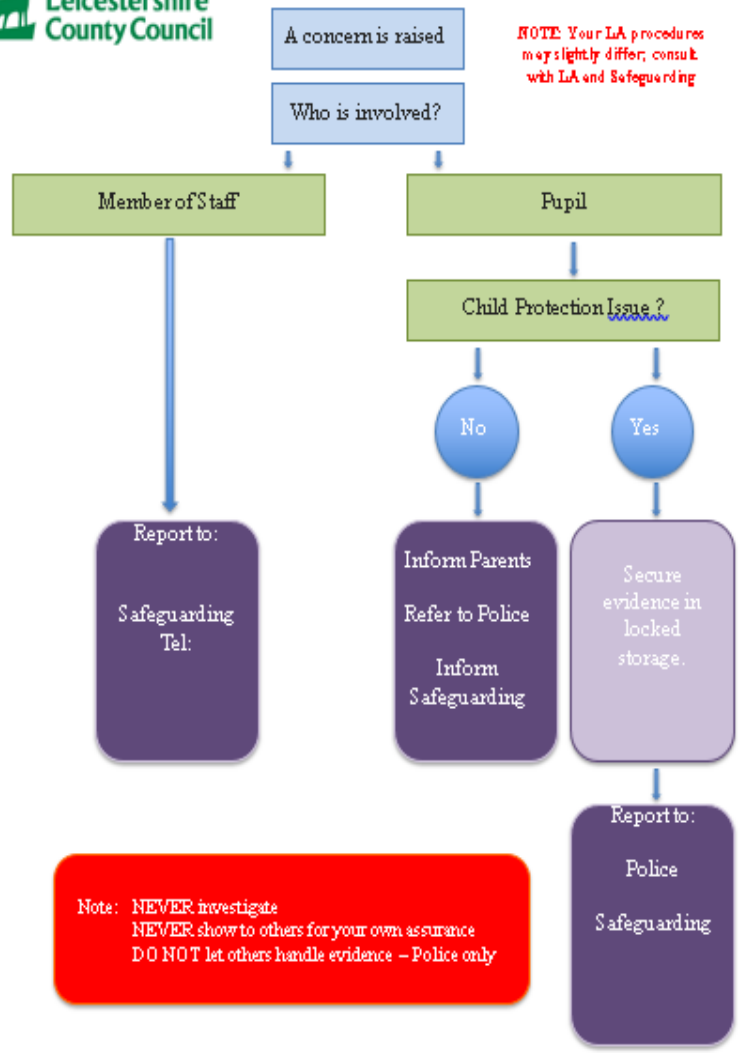
Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
Likelihood 3	Children/young people's inquisitive nature is that they may actively seek out unsavoury online content, or come across such content accidentally. Likelihood is therefore 3
Impact 3	The impact to the school reputation would be high. Furthermore school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	Online Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The Online Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school Online Safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Inappropriate Activity Flowchart



Illegal Activity Flowchart

Leicestershire County Council



Our Charter of Good Online Behaviour (for 2018 onwards)

Note: All Internet, email and PC activity may be subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment, if I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anybody asks me for personal information.

I will – let my teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will – be respectful to everybody online ; I will treat everybody the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter there will be consequences of my actions and my parents will be told.

Signed (Parent) :

Signed (Student) :

Date :