Buckstones Community Primary School

E-Safety & Acceptable Use Policy

Written by staff: Monday 20th. March 2017
Approved by Governors on: 28.3.17

E-SAFETY POLICY – 1

MISSION STATEMENT

At Buckstones School, we aim to promote the development of our children academically, physically, socially, morally and spiritually, by providing a high quality of teaching and varied learning experiences within a well-ordered and stimulating environment, which supports equality of opportunity.

We teach the National Curriculum, planning for and presenting the children with challenges that support differentiation.

We aim to nurture individual skills and talents within an environment which values, self worth, confidence, independence, self-motivation and co-operation, and in which our children have respect for each other's differences.

We aim to give our children a love of life and learning.

1.0 Introduction

The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect pupils from potential and known risks

The school has appointed an e–Safety Lead Mrs Nicola Leigh. Our e–Safety Policy has been written by the school, building on advice from OLSCB and government guidance.

The focus for this policy is to ensure that existing policies (such as those on child protection, anti-bullying, the curriculum and behaviour) are applied to the digital environment. In order for this to happen, these policies are regularly reviewed against the Local Authority's and national guidance, and updated as necessary.

This policy covers:
•Managing on-line technology so that pupils are kept as safe as possible.
•The responses necessary when a risk to a child is discovered

Safeguarding pupils, including e-safety is everyone's responsibility. E-safety is therefore not just the responsibility of the e–Safety Coordinator, the Computing Subject Leader, the Headteacher or the IT Technician.

The overall aims of this policy are to ensure that pupils:

- Are equipped to assess risks in a digital environment.
- Are enabled to make informed judgements about such risk.
- Know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact).

2.0 Teaching and Learning

Whilst recognising the considerable benefits of new technologies, we teach pupils to protect themselves from:

- inappropriate content

- undesirable contact
- hurtful conduct

Research indicates that pupils who are given greater freedom at school to use new technologies have a better knowledge and understanding of how to stay safe online. It is therefore important that this school runs a 'managed system' that helps pupils to become safe and responsible users of technology by allowing them to take more responsibility and manage their own risk. We believe that pupils become more vulnerable if they are not given the opportunity to learn how to assess and deal with online risk for themselves.
To support this, the school has adopted the Oldham Charter of Young People's Digital Rights and this is shared widely with pupils in all classes. (See Appendix 2)

2.1 Why use on-line technology?

- The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and students.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 How does on-line technology enhance learning?

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Pupils are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.
Different ways of accessing information from the Internet will be used depending upon the nature of the material being accessed and the age of the pupils.

- Access to the Internet may be by teacher or teaching assistant demonstration.
- Pupils may access teacher-prepared materials through the shared folder on the school server or school Intranet, rather than the open Internet.
- Pupils may be given a suitable web page or a single website to access.
- Pupils may be provided with lists of relevant and suitable websites.
- Older, more experienced pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher. Pupils will be expected to observe the rules for acceptable use.

Pupils accessing the Internet will be supervised by an adult at all times.

2.3 Pupils will be taught to evaluate Internet content

We believe that, in order to use information from the Internet effectively, it is important for pupils to develop an understanding of the nature of the Internet and the information available on it. In particular, they should know that most of the information on the Internet is intended for an adult audience and that much of the information on the Internet is not properly audited/edited. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- Pupils will be taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV.

- Teachers will ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the Internet (as a non-moderated medium).
- When copying materials from the Internet, pupils will be taught to observe copyright.
- Pupils will be made aware that the writer of an e-mail or the author of a webpage may not be the person claimed.

2.4 E-safety education / curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Pupils need the help and support of the school to recognise and avoid e-safety risks and build their resilience. They also need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. (See appendix 4)
- Staff and volunteers should act as good role models in their use of digital and online technologies and are required to sign an Acceptable Use Agreement. (See appendix 3)
- 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, staff should be vigilant in monitoring the content of the websites the young people visit.

2.5 Parents / Carers

Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours yet many have a limited understanding of e-safety risks and issues. Parents may under estimate how often their children come across potentially harmful and inappropriate material on the Internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,

- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

(See Appendix 9 - Governor Advice Leaflet on E-safety)

3.0 Managing the use of on-line technology

3.1 Acceptable Use Policy (AUP)

This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The AUP details how we provide support and guidance to parents / carers for the safe and responsible use of these technologies by adults and pupils

In order to prevent inappropriate situations occurring it is important that staff, volunteers and pupils are aware of their responsibilities and the expectations whilst using technology. Each user signs a contract to ensure that they know what is deemed 'acceptable use of the Internet'. (See appendices 3&4).

3.2 The e-safety Lead

At Buckstones Community Primary School the e-safety lead works closely with the designated person for Child Protection. Mrs Nicola Leigh is the school's e-safety lead and Miss Sarah Healey (Headteacher) is the school's designated person for Child Protection. The responsibilities of the lead person include:

- Updating the AUP
- Ensuring that policies and procedures include aspects of e-safety for example the anti-bullying policy includes cyber-bullying
- Working with the ICT Technician to ensure that filtering is set at the correct level for staff and pupils.
- Ensuring that staff training is provided on e-safety issues
- Ensuring that e-safety is included in staff induction
- Monitoring and evaluating incidents that occur to inform future safeguarding

3.3 Password Security

For pupils to access the school network there is a general 'log in' for each year group. This gives access to the Internet and a variety of software. All work is saved directly onto the school server. Pupils do have their own log in and passwords for Spag.com and 'Purple Mash' which they are taught to keep secret and not to share with others. Pupils are instructed to inform their teacher if they think their password has been compromised or someone else has become aware of their password.

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. Staff are regularly reminded of the need for password security. Staff should ensure that computers and laptops are not left unattended and are always locked when not in use.

- Staff are instructed to inform the e-safety lead if they think their password has been compromised or someone else has become aware of their password.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS and Learning Platform. Including ensuring

that passwords are not shared and are changed periodically.
- Staff should ensure that computers and laptops are password protected and not left unattended.
- All work, data and images stored on portable devices must be password protected / encrypted.

3.4 Managing Specific on-line Technologies

3.4.1 Internet Access

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form for their child to use the Internet

- At Key Stage 1, access to the Internet will be by adult demonstration and direct supervised access to specific, approved on-line materials
- At Key Stage 2, pupils will work independently using the Internet, but will not be left unsupervised.
- Parents will be asked to sign and return a consent form (see AUP)

3.4.2 Email

- E-mailing is currently restricted to communication within the school.
- Pupils are instructed to tell a teacher if they receive offensive email.
- Pupils cannot send messages to external organisations. These have to be sent through the teacher's First Class Account.

3.4.3 The school website:

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Website photographs that include pupils will be selected carefully with the agreement of parents / carers.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.

3.4.4 Chat and instant messaging

- Pupils will not be allowed access to public or unregulated chat rooms.
- Pupils will not access social networking sites for example 'Facebook' or 'Instagram'.
- Pupils should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.
- Any form of bullying or harassment is strictly forbidden.

3.4.5 Filtering

- The School works in partnership with parents, the LA, Internet Service Provider and DFE to ensure that systems are in place to protect pupils.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Local Authority via the e-safety lead.
- Any material that the school believes to be illegal must be referred to the Internet Watch Foundation (IWF)

3.4.6 Photographic, video and audio technology

- It is not appropriate to use photographic or video devices in changing rooms or toilets.
- Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.
- Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. School equipment should be used for this purpose. Should personal equipment ever be used, then all images must be transferred to school hardware and deleted from the personal device as a matter of urgency.
- Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
- Pupils should always seek the permission of their teacher before making audio or video recordings within school grounds.

This guidance around images applies also to moving images – i.e. video and video links. Care should be taken with the security of video files on computers, servers, and portable drives, as well as those remaining on a video camera after use. Any copies unsecured (e.g. on the video camera itself) should be deleted.

3.4.7 Mobile Phones/Devices

- The sending of abusive or inappropriate text messages is strictly forbidden.
- Pupils are allowed mobile phones in school, however, they must be switched off and the school takes no responsibility for loss, theft or damage (see Mobile Phone Policy). However it is recognised that for older pupils some parents / carers may wish them to have a mobile phone with them if they walk to/from school on their own. Staff must have their mobile phones switched off during teaching time.
- Signage instructs all visitors to turn off their mobile phones when coming onto the premises to prevent any images being recorded.
- All professionals working with young people who use personal mobile devices should ensure that they have an appropriate pass code set to prevent access by anyone who has taken the device. Similarly, passwords for email and other online services should not be saved on the device.
- Mobile devices should not be used to store pupil's personal data. It is perfectly reasonable and normal for teachers, for example, to have spreadsheets of assessment data, targets, etc that they use for monitoring and analysis but not personal data (such as home addresses, contact telephone numbers, medical information, photographs etc) which should never be needed on such a device.
- Sexting is where young people share sexual messages and images of themselves or others.
  This act itself poses a risk to the young person in the image: once it has been shared it is liable to be distributed further. This action may also place both the sender and the recipient in a position of having committed an offence under the Protection of Children Act 1978.Young people of an age likely to consider such actions should be educated about the risks.

3.4.8 Emerging ICT Applications

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

4.0 Complaints regarding the use of on-line technology

Prompt action is required if a complaint is made. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School's Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Oldham LSCB child protection procedures.
Any complaints about staff misuse of on-line technology must be referred directly to the Headteacher.

The responses necessary when a risk to a child is discovered.

Prompt action is required if a complaint is made regarding the use of on-line technology. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Oldham LSCB child protection procedures.

Any complaints about staff misuse of on-line technology must be referred directly to the Headteacher.

5.0 How to respond when a risk is discovered

The e-safety lead will ensure that the following procedures are adhered to in the event of any misuse of the Internet:

5.1 An inappropriate website is accessed inadvertently:

- Report website to the Headteacher and e-safety lead.
- Contact the filtering service so that the site can be added to the banned or restricted list.
- Log the incident. (See appendix 5)

5.2 An inappropriate website is accessed deliberately:

- Ensure that no one else can access the material by shutting down the computer.
- Log the incident.
- Report to the Headteacher and e-Safety lead immediately.
- Manager to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
- Inform the filtering services as with 5.1 in order to reassess the filters.

5.3 An inappropriate website is accessed deliberately by a child:

- Refer the child to the Acceptable Use Rules that were agreed.
- Reinforce the knowledge that it is illegal to access certain images and police can be informed.
- Log the incident
- Decide on appropriate sanction.

- Notify the parent / carer.
- Contact the filtering service to notify them of the website.

5.4 An adult receives inappropriate material:

- Do not forward this material to anyone else – doing so could be an illegal activity.
- Alert the Headteacher and e-Safety lead immediately.
- Ensure the device is removed and log the nature of the material.
- Contact relevant authorities for further advice e.g. police, social care, CEOP.
- Log the incident.

5.5 An illegal website is accessed or illegal material is found on a computer.

5.5.1 The following incidents must be reported directly to the police:

- Indecent images of pupils found. (Images of pupils whether they are photographs or cartoons of pupils or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.
- Criminally racist or anti-religious material
- Violent or bomb-making material
- Extremism and radicalisation material (refer to The Prevent Duty)
- Software piracy
- The promotion of illegal drug-taking
- Adult material that potentially breaches the obscene publications act in the UK.
- Harrassment

5.5.2 If any of these are found, the following should occur:

- Alert the Headteacher and e-Safety lead immediately.
- DO NOT LOG OFF the computer but disconnect from the electricity supply.
- Contact the police and or CEOP/ Channel and social care immediately (Police – 0161 856 8962, social care – 0161 770 3790, pupils over 16 – 0161 770 6599, out of hours – 0161 770 6936).
- If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

5.6 **An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)**

- Ensure the child is reassured and remove them from the situation.
- Report to the manager and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures www.oldham.gov.uk/lscbhome
- Report to the Local Authority Designated Officer (07515188790).
- Preserve the information received by the child if possible.
- Contact the police as necessary.

5.7 **Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:**

- Preserve any evidence and log the incident.
- Inform the Headteacher immediately and follow Child Protection Policy.
- Inform the e-Safety Leader so that new risks can be identified.
- Contact the police or CEOP if appropriate.

5.8 **Where staff or adults have posted on inappropriate websites, or have inappropriate information about them posted:**

- This should be reported to the Headteacher.

5.9 **Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying)**

- Preserve any evidence and log the incident.
- Inform the Headteacher and e-Safety lead immediately.
- Check the filter if an Internet based website issue.
- Contact/parents and carers
- Refer to the bullying policy
- Contact the police or CEOP as necessary.

5.10 If images or video of pupils engaged in sexual activity or in revealing poses (sexting) are known to have been posted online the following guidelines should be followed:

- If the images are on a computer follow the guidelines for inappropriate use of ICT equipment. Where the existence of the video or images has come to attention through young people talking about them or viewing them on their phones the following measures should be taken then the Police should be contacted immediately and a CEOP report made giving the available information.
- The incident should be logged through the organisation's own monitoring / line management procedures.
- Appropriate educational/pastoral work should be undertaken with all young people involved.

Introducing the policy to pupils

•Rules for acceptable use will be posted in all rooms where computers are used.
•Pupils will be informed that Internet use will be monitored.
•Instruction in responsible and safe use should precede Internet access.
•A module on responsible Internet use will be included in the PSHE programme covering both school and home use.
•Oldham's youth charter will be displayed. (See appendix 2)

Introducing the policy to staff and volunteers

•All staff and volunteers must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
•All staff including teachers, supply staff, classroom assistants, administration and caretaking staff, and Governors will be provided with the School Internet Policy, and its importance explained.

•Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
•The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
•Staff development in safe and responsible Internet use, including familiarisation of the E-safety and acceptable use policy will be provided as required.

Maintaining ICT system security
•The school ICT systems will be reviewed regularly with regard to security.
•Virus protection will be installed and updated regularly.
•Security strategies will be discussed with the LA/IT service provider.
•Personal data sent over the Internet will be encrypted or otherwise secured.
•Use of portable media such as memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
•Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
•Files held on the school's network will be regularly checked.
•The ICT subject lead / ICT technician will ensure that the system has the capacity to take increased traffic caused by Internet use.

REVIEW OF POLICY:

These policies are regularly reviewed against this e-safety guidance, and updated as necessary and in line with the Policy Management Cycle

Appendix 1

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities 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 Governors receiving regular information about e-safety incidents. The Governors role will include:

- updates/ reports from the E-Safety Lead
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher and (at least) 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.
- The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

E-Safety Lead:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policy / 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 / relevant body.
- Liaises with school technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- Updates Governors to discuss current issues and review incident logs.
- Reports to Senior Leadership Team.
- Organises E safety week and Information events and keeps parents fully informed

Network Manager / Technical staff:
The IT technician is responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- That the school meets required e-safety technical requirements.

- That users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- That they keep 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.
- That the use of the network / Internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / e-safety lead.

Teaching and Support Staff Teaching and support staff are responsible for ensuring 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 Staff Acceptable Use Agreement
- They report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- All digital communications with pupils / parents / carers 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 activities.
- Pupils understand and follow the e-safety and acceptable use policies.
- They monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
- 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.

Child Protection / Safeguarding Designated Person

The Child Protection Officer for the school should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding 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.

Pupils:

- Are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- 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.
- Know and understand policies on the taking / use of images and on cyber-bullying.
- 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 pupils understand the need to use the Internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog
- their pupil's personal devices in the school (where this is allowed)

Appendix 2

Oldham Charter of Young People's Digital Rights

Charter of Young People's Digital Rights

oldham Youth Council

1. You have the right to enjoy the internet and all the fun and safe things it has to offer.
2. You have a right to keep information about you private. You only have to tell people what you really want them to know.
3. You have a right to explore the internet but remember that you cannot trust everything that you see or read on the internet.
4. You have a right to know who you are talking to on the internet; you don't have to talk to someone if you don't want to.
5. Remember not everyone is who they say they are on the internet. You have a right to tell someone if you think anyone is suspicious.
6. You have a right NOT to fill out forms or not to answer questions you find on the Internet.
7. You have the right to NOT be videoed or photographed by anyone using cameras, web cams or mobile phones.
8. You have a right NOT to have any videos or images of yourself put on the Internet, and you have the right to report it to an adult if anyone does this.
9. You have a right NOT to be bullied by others on the Internet and you have the right to report this to an adult if this happens.
10. If you accidentally see something you shouldn't you have the right to tell someone and not to feel guilty about it.
11. We are ALL responsible for treating everyone on line with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

Oldham Youth Council 2008 - 2009

Launched in Oldham eSafety Week 2009. For more information and the interactive version of this charter, go to ***www.e-safetyweek.info***

Appendix 3

Contract for Acceptable Use of the Internet (Staff/Volunteer)

I know that I should only use school equipment in an appropriate manner.

I know that images should not be inappropriate or reveal any personal information of pupils and young people if uploading to the Internet.

I have read the school e-safety and acceptable use policy so that I can deal effectively with any problems that may arise.

I will report accidental misuse to the Headteacher.

I will report any incidents of concern for the pupil's safety to the Headteacher, designated person for child protection in accordance with the e-safety and acceptable use policy.

I know the designated person for child protection is Sarah Healey and in her absence Melanie Platt.

I will ensure that personal data (such as data held on SIMS) is kept secure and I follow the Data Protection Act 1998.

I know that I am putting myself at risk of misinterpretation and allegation if I contact pupils and young people via personal technologies, including my personal e-mail and phone and should use the school e-mail and phones (if provided) and only to a child's school e-mail address if possible .

I will ensure that I keep my password secure and do not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password I will check with the e-Safety Leader.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will ensure that al electronic communications with pupils and staff are compatible with my professional role.

Name: ……..

Signed: ……..

Position: ……Date: ……..

Appendix 4

Contract for Acceptable Use of the Internet (Pupil)

These rules help us to be fair to others and keep everyone safe.

I will ask permission before using the Internet.

I understand that I must not bring software or disks into school without permission.

I will only email people that my teacher has approved.

The messages that I send will be polite and sensible.

I understand that I must never give out my home address or telephone number, or arrange to meet someone.

I understand that I must ask for permission before opening an email or an email attachment sent by someone I do not know.

I will not use Internet chat.

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

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

I understand that if I deliberately break the rules, I may not be allowed to use the Internet or computers.

Date: ……
The undersigned have read and agreed to the above.

Appendix 5

Incident log sheet

Inappropriate Internet Use Incident Log

Person reporting incident:

Date: Time:

Nature of incident: (Keep factual: Who? What? Where? When?)	
Actions Agreed and by whom	**Contact** eg telephone calls made etc

Signed by adult raising the concern: ……

Signed by E-safety Lead: ……..

Appendix 6

Information and websites about e-safety.

CEOP

- http://www.ceop.gov.uk

Think U Know

- http://www.thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1

Becta

- http://localauthorities.becta.org.uk/index.php?section=esf

Childnet

- http://www.childnet-int.org

Internet Watch Foundation

- http://www.iwf.org.uk

BBC

- http://www.bbc.co.uk/cbbc/help/web/staysafe

Appendix 7

Buckstones Community Primary School guidance note on privacy settings within social media sites and apps.

This document is intended as a guidance note on "how to" maintain your privacy within the "top 3" social media environments readily used by people on a day to day basis and is a **supplementary note to the Safer Working Practices Policy – specifically section *"4.5 relating to Social Contact and Social Networking".*** The note is based on advice and guidance from a few different sources including the NASUWT and the University of Sussex.

Facebook

Facebook is the number one social media site platform across the world. As of the second quarter in 2015, Facebook has just under 1.5 billion active users, of which over 1 billion use on a monthly basis at least. The points below are suggested guidance on how to maintain a level of privacy with a Facebook profile and the information contained within it.

It should be noted that the legal minimum age to have a Facebook profile within the UK is **13**.

The NASUWT recommend that:

1. To ensure that your Facebook account does not compromise your professional position, please ensure that your privacy settings are set correctly (see below)
2. Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your school.
3. Always make sure that you log out of Facebook after using it, particularly when using a machine that is shared. Your account can be hijacked by others if you remain logged in – even if you quit your browser and/or switch the machine off. Similarly, Facebook's instant chat facility caches conversations that can be viewed later on. Make sure you clear your chat history on Facebook (click "Clear Chat history" in the chat window).

To maintain your privacy, they recommend the following settings are enabled: **NB: If you choose to enable any or all of the recommendations described below, this must be done in the web version of Facebook, NOT via the smartphone/tablet app.**

Privacy Setting	Recommended Security Level
Send you messages	Friends only
See your friend list	Friends only
See your education and work	Friends only
See your current city and hometown	Friends only
See your likes, activities and other connections	Friends only
Your status, photos, and posts	Friends only
Bio and favourite quotations	Friends only
Family and relationships	Friends only
Photos and videos you're tagged in	Friends only
Religious and political views	Friends only
Birthday	Friends only
Permission to comment on your posts	Friends only
Places you check in to	Friends only
Contact information	Friends only

E-SAFETY POLICY – 1

Even when the privacy settings are set to 'friends only', you might be surprised to see some information still readily available to the public via a "Google" search on your name and then people still being able to link to your Facebook profile and view:

1. previous posts (pre-privacy settings)
2. previous Facebook banners
3. your friends block
4. groups you have recently joined
5. your relationship status (if published)
6. the 'about you' block
7. recent activity

In order to prevent this, the University of Sussex recommend applying the following additional privacy settings:

1. Go to **Settings**
2. Select **Privacy**
3. Change all of your posts to be available **only to friends** (as described above)
4. Set **'delete past posts'** to ensure posts that were public before your settings changed are deleted from your timeline.
5. Then go to **Manage Sections.** You will find this in the top toolbar. Untick all of the options so that no blocks are available for public viewing.
6. And finally…go to your photo block (and other blocks including groups block, friends block, etc) and click on the **edit pencil** and select **hide**.

Last thing, make sure your banner and your personal profile picture is an image with information that you wish to share. No matter what your settings, **these two images will be available at all times.**

If you choose to apply these settings, you can check how your profile will appear once this is completed by:

1. go to settings
2. go to **view as**
3. select 'public' view

This will provide you with a view of your profile as it will appear to someone how finds you within a "Google" search and how is not currently within your "Facebook Friends List".

It's useful to note that Facebook changes its privacy settings from time to time so what might have been private yesterday could be public tomorrow. A new feature was added by Facebook on the 17th of September; a friendly dinosaur that can help you with your privacy settings, available under your privacy shortcut.

E-SAFETY POLICY – 1

Instagram

Instagram is the second most used social media platform across the globe with a disclosed total number of 400 million active users, of which 75 million use the platform on a day to day basis. Like Twitter, by default an Instagram profile is "public" – i.e. whatever images you post can be seen by any other Instagram user (whether you have approved them as a follower or not) or via a simple search on the internet.

Like Facebook, Instagram does have a legal minimum age of 13.

The notes below provide some guidance/pointers on how to enable a level of security on your Instagram profile. **NB: these changes can [and should] be applied via the Instagram app, unlike Facebook and Twitter.**

1. Open the Instagram app on your smartphone or tablet.
2. Go to your profile by touching the "person" button in the lower right-hand corner.
3. Touch the "wheel" (or "cog") image in the top right of your screen.
4. Under the account section, Switch to On the "Private Account" setting.
5. Upon clicking Instagram will ask for confirmation.
6. Confirm it by touching "YES".

From now on anyone who wants to see your Instagram photos has to send you a follow request which will appear in the news feed. To check who has requested to follow you and either approve or ignore, then:

7. Go to the news/activity feed by clicking the feed icon on the bottom [A speech bubble with a heart inside it].
8. You will reach the news/activity feed where you'll see a "follow requests" section at the top.
9. If you have multiple requests, the number will be displayed and on clicking on this, a list will form.
10. You can then "approve" [Green Tick] or "ignore" [Red Cross] each request.
11. If you have a single request, the "approve" or "ignore" options will appear directly within the news/activity feed.

Linking Instagram to other social media platforms.

Some websites, social networks and apps give you the option to sign in or to verify your identity by linking your account to their service. Whilst this is OK, you should be aware that you're giving the third party (the website, social network or app) access to your Instagram username, your lists of followers, who you are following, and your location (if you share it) and your posts - even if you've set them to "Private".

Twitter

Twitter is the third most used social media platform across the world and has a significantly smaller user base across the planet – as at the end of Sept 2015, it had 232 million active users. By default, a Twitter profile is "public" – i.e. whatever you tweet can be seen by any other Twitter user (whether you have approved them as a follower or not) or via a simple search on the internet. The notes below provide some guidance/pointers on how to enable a level of security on your Twitter profile.

Unlike Facebook & Instagram, there is NO legal minimum age for the use of Twitter, but the recommended minimum age is 13. Your date of birth is not required to create a Twitter account.

It should be noted that by making your profile and Tweets private the following will apply:

1. Other users will need to make a request to follow you, and you will need to approve all requests.
2. Your tweets will only be visible to approved followers.
3. Other users will be unable to retweet you.
4. Your tweets will not appear in any Google searches, and will only appear in Twitter searches conducted by your approved followers.
5. Any @replies you send will not be seen, unless you send them to your approved followers. For example, if you tweet a celebrity they will not be able to see it, unless you have approved them to follow you.
6. Anything you tweeted while your account was public will now become private, and will only be viewable or searchable by your approved followers.
7. You will only be able to share permanent links to your tweets with your approved followers.

If you wish to enable privacy on your Twitter account (which is recommended) then the following steps need to be applied via the webpage version of your account:

- Log in to your Twitter account with your username and password and click on your profile picture and select “settings”. Under settings, select “security and privacy”. **Then click [check] the following boxes:**
    - **Photo Tagging:** Do not allow anyone to tag me in photos
      Though others can still upload photos of you, you now can't be publicly tagged in them.
    - **Tweet Privacy:** Protect My Tweets
      People will now need your permission before they can follow you (though you will keep all the followers you have now). Future tweets will only be visible to your followers, no-on can retweet your tweets, and your tweets will not show up in Google search results Limitations: you can't reply to tweets posted by non-followers. **Note:** this only works on future tweets; all past tweets will still be public.
    - **Discoverability**: Let others find me by my email address
      People now can't find your Twitter account by searching your email address. This is especially if you do not want your email address publicly linked to your account.

Linking Twitter to other social media platforms.

As with Instagram, you can link or share your Tweets via other social media platforms, however, the same cautionary note applies, in that you're giving the third party (the website, social network or app) access to your Twitter username, your lists of followers and following, and your location (if you share it) and your tweets - even if you've set them to "Private". You will also be giving Twitter information about the other services that you use.

With all this in place finally think about the content of what you post, any content should not bring the school or the profession into disrepute.

Appendix 8
Policy and Guidance for adults using First Class

General
1. First Class is provided for Oldham schools and Local Authority users by the Local Authority. As such its use is governed by relevant policies adhered to by the Authority, including the Data Security policy, the Personal Use of the Internet policy (especially section three, e-mail), and the LSCB eSafety policy.
2. All schools and other users of the First Class system are expected to ensure that their staff are aware of these guidelines and that any breaches are acted on appropriately.

Access to First Class
3. First Class accounts are created by the Local Authority's Learning & Achievement ICT Technical Support Team. Schools and other users requiring additional accounts to be created should contact this team (contact details are provided in paragraphs 29-30 of this document). Schools take the responsibility to ensure that accounts are requested only for appropriate users. Accounts should be requested only for pupils or for adults with current CRB clearance who are employed to work in the school or have a formal role in relation to it such as school governor.
4. Schools and other users should inform the team, in the same way as above, of staff leaving their establishment for accounts to be deleted or transferred to a different establishment (both for security purposes and to avoid a continuing cost for the account). Under no circumstances should an ex-member of staff be allowed to continue to use an account associated with their former school.
5. Unlike e-mail accounts with the oldham.gov.uk suffix, First Class accounts can be created for people who are not council elected members or employees, such as school governors, children and generic accounts for classes. The safe and proper use of these accounts remains the responsibility of the establishment or Local Authority Service that has requested their creation.
6. Where schools request it, limited additional rights may be given to a member of staff in school such as an IT technician, administrator or ICT Co-ordinator to enable them to perform certain actions for users within the school. This member of staff could be anyone nominated by the school. Such requests can be made in the same way as a request for a new account as above.
7. In exceptional circumstances such rights may be given to staff externally contracted for ICT support, but this will only be on receipt of an up to date CRB clearance for the person concerned, a signed copy of this policy indicating that they are aware of and understand the terms on which those rights are given, and an indication from the schools governing body that they are taking responsibility for this person's use in the same way as they do for staff and children.

Data Security
8. All users of First Class should be aware that no e-mail system is entirely secure and that great care should be taken with any sensitive information sent by e-mail. In particular, sensitive data (including personal details relating to children such as home address, medical or social care information) should never be sent or copied to any external e-mail address from First Class, unless strongly encrypted.
9. The Oldham First Class system is hosted within the Local Authority and as such e-mails sent within this system (i.e. from one Oldham First Class user to another) are more secure

than those sent externally. Email sent between Oldham First Class and @oldham.gov.uk e-mail addresses may also be considered to be internal.

10. Sensitive data sent even by such internal email should be addressed only to a single recipient. Caution should be exercised with such data and consideration should be given to whether it would be sensible to password-protect attached files.

11. All users of First Class are expected to ensure that their password security is maintained. Passwords should not be written down, and should not be simple words (particularly obvious things such as a surname, the name of a child or a family pet, or the word password). Advice on how to create easy-to-use yet secure passwords can be obtained from the Local Authority's Learning & Achievement ICT Technical Support Team. (Users should note that new First Class accounts are created with simple passwords – this password should be changed to a new complex password at first log-on).

12. Under no circumstances should any user give their password to anyone else or allow anyone else to use their First Class account. Where a member of staff requires access to another person's account (during a long-term absence of a senior member of staff, for example) a formal request for a temporary account change should be made by the school or service).

13. Users should be cautious about the use of the First Class client's ability to save a password and thus auto-log-in. This should never be set on any shared (or potentially shared) computer that does not have a password required on start-up. Many mobile devices (such as iPhones) also include such an auto-save feature; this should be disabled or a passkey used with the device to protect the users e-mail security in the event of loss or theft.

14. Under no circumstances should anyone log in to First Class as anyone else.

Email and the Law

15. Email is a formal communication admissible in a court of law and potentially subject to release if requested under Freedom of Information legislation. All users of First Class should be aware that their emails or other messages may be interpreted by others (including those to whom a message has been forwarded on) in a different way to that intended.

16. Users should ensure that messages within or from First Class are not open to interpretation as constituting orders for products or services. (For example, an email from a school e-mail address requesting goods to be delivered to the school may constitute an order from the school, even if intended to be personal).

17.Users should ensure that messages within or from First Class are not in any way defamatory, abusive, discriminatory or in any other way likely to be in breach of the council's or school's legal obligations or bring the council or school into disrepute.

Accounts for Children

18. First Class accounts may be created for children or classes within a school by decision of the school's governing body (or decision of that Governing Body to delegate this authority to the Headteacher).

19. Where such accounts are created, those accounts will have limited rights (e.g. being unable to see accounts outside of their school or setting within the First Class directory). Schools should nevertheless regularly check such accounts to ensure that they are not being abused, or children being abused through their use.

20. Wherever a school makes use of such accounts, the school is expected to ensure that its teaching of e-safety takes place also within the context of the use of First Class. (Advice about eSafety and how to teach it in school can be obtained from CLC, which leads on this work on behalf of the LSCB).

Other Guidelines

21. FirstClass includes many features that are valuable in communication, personal organisation, teaching and professional dialogue. Training on the use of First Class, if required, is available from the CLC in collaboration with the ICT Technical Support Team.
22. Users should ensure that First Class is accessed only from properly maintained devices, with up to-date anti-virus protection for example. Users should be careful not to forward any messages containing dangerous attachments or links to dangerous files stored elsewhere.
23. If it is ever necessary to put a limit on the size of large attachments sent through First Class this limit will be announced through the all users conference.
24. If any message received is clearly intended for someone other than the addressed recipient the user should inform the sender and delete the message.
25. If any activity within the First Class system causes concern of an operational or technical nature please contact the Local Authority's Learning & Achievement ICT Technical Support Team as detailed at the end of this document.

Administration within the Local Authority

26. In order to ensure the reliability and security of the overall system, the LA will keep records of the accounts created, deleted and modified and copies of the requests from schools to do so.
27. This policy may be amended from time to time (by agreement of the ICT Strategy Group) as technology and users' needs develop. An up-to-date copy will always be available in the Policies conference within First Class.
28. The LA reserve the right to suspend any account suspected of being misused, subject to notification to the user concerned and further investigation.
29. All contact with the Local Authority's Learning & Achievement ICT Technical Support Team to request new First Class accounts, or the deletion or modification of accounts should be made within the First Class system from a Headteacher's account to fcadmin@oldhamlea.org.uk
30. For other First Class enquiries please either email fcadmin@oldhamlea.org.uk, contact fcadmin@oldhamlea.org.uk through First Class or ring 0161-770 3678.
31. In order to guarantee security within First Class, the control of passwords for full administrative access will comply fully with standard industry practice, with access to these passwords tightly restricted. Access to the reduced administrative accounts required for day-to-day system management is also controlled and restricted to a small number of key users. Details are available from fcadmin@oldhamlea.org.uk or the Unity Service Desk on 0161-770 1000.

Policy for Adoption by School Governing Bodies

First Class is provided for Oldham schools by the Local Authority to facilitate communication and professional dialogue within and between Oldham schools. In the interests of safe and secure use and development of the system, the Local Authority is requesting that Governing Bodies of schools using First Class adopt this policy with regard to its use.

1. Buckstones Primary School uses the LA-provided e-mail and conferencing system First Class in accordance with the terms of use contained in the appended document The Oldham First Class Communication System provided by Oldham Council - Policy and Guidelines for Use.
2. Use of First Class by staff will be in accordance with these guidelines.
3. The Governing Body has delegated to the Headteacher decisions about whether or not First Class accounts are provided by the school for its pupils.
4. The school does not currently request First Class accounts for any adults other than those directly employed by the school.

Appendix 9

Parents leaflet about e-safety

This short guide has been put together for parents to help them make aware of some controls they can add to mobile devices to make them safer for their children to use.

There is a lot of information on the Internet, but often this is overlooked until it is too late. We have gathered some useful hints and tips for both the iPhone, iPod and iPad (iOS devices) and Samsung Galaxy, Google Nexus, Hudl and other Android devices as well as personal information and online gaming.

Making Tablets Safe

E-SAFETY POLICY – 1

Personal Information
Regardless of the device you have most users have a lot of personal information stored on their devices, including photos and videos, and they may also have automatic logins set up for email, social networking and bank accounts.

Set a passcode
It is always a good idea to set a Passcode, so that if someone does steal or find your iPad then they can't access any personal information you may have stored on it.

iOS (iPhone, iPad, Ipod)

In Settings select General. Then select Passcode Lock.

Android (Samsung Galaxy, Google Nexus etc..)

In most Android devices similar settings can be found under the **Settings > Security** menu

You can also select how long your device should wait before locking. By selecting Erase Data your device will delete all data after ten attempts at the passcode (although young people may wish to switch this Off if they are worried friends might do this as a prank!).

Online Gaming

Online gaming is hugely popular with children and young people. Recent research shows that gaming is one of the top activities enjoyed by 9-16 year olds online, with gaming more popular than social networking.
From sport related games to mission based games and quests inspiring users to complete challenges, interactive games cater for a wide range of interests, and can enable users to link up and play together.

Tips

It may seem daunting, but one of the best things parents and carers can do is to engage with the gaming environment and begin to understand what makes it is so attractive to young people as well as the types of activities that they enjoy!	**Talk with your children about the types of game(s) they are playing. Are they role-playing games, sports games, strategy games or first person shooters? If you're not sure what they are, ask them to show you how they play and have a go yourself.**
Some games may offer children the chance to chat with other players by voice and text. Ask them who they are playing with and find out if they are talking to other players. If chat is available, look at the type of language that is used by other players.	Remember that the same safety rules for surfing the net apply to playing games on the internet.

iPhone, iPod and iPads

Settings

There are a number of settings that can improve the safety of your child using an iPhone, iPod or iPad.
These can be found under the

Settings > General > Restrictions menu.
You can:

- Turn off access to certain apps (Safari, YouTube)
- Remove the ability to download explicit content for music
- Set ratings for downloading movies or TV shows
- Set volume limits

Internet Browsing

It's a shame for an inquisitive mind to have to cut access to the internet entirely, but offering web access is a huge worry.

You can use 'child safe' internet browsers, an example is **Ranger Pro Safe Browser**.

It's free and quick to register the required web account, from which you can monitor and manage allowed web site content at **mobsafety.com**.

Prevent 'in-app purchases

In-app purchases often occur in games, but young people may not be aware this is a 'real money' purchase. You will be asked to enter your iTunes Store Account password to make an in-app purchase.
To prevent in-app purchases go to the **Settings > General > Restrictions** select Off for In-App Purchases.

Read Apple's advice about iPad parental restrictions: http://support.apple.com/kb/ht4213

THINK U KNOW .CO.UK

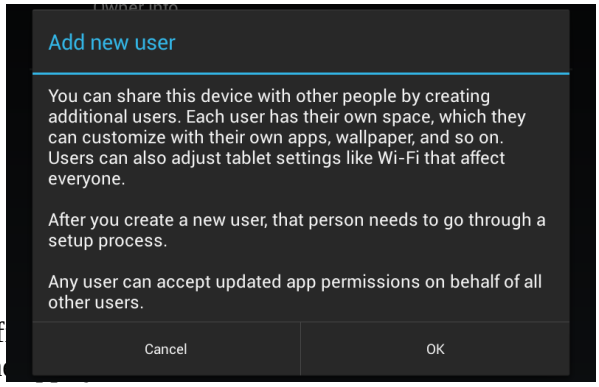
This is a great web page giving advice to different age groups, parents/carers and teachers about using the Internet safely.

This also contains info on how REPORT ABUSE

Android Tablets and Smart

Android tablets and smart phones are becoming increasingly popular and that means that your child may get their hands on one of them at some point.
Even the latest version of the Android operating system does not have any comprehensive parental controls, but there are steps you can take to make your device safer for your child to use.

Set up a user account



If you are running Android version 4.2 or later you can configure multiple user accounts that can have different restrictions applied to them.
You can do this by going to settings. Scroll down to and select Users, then tap 'Add user or profile'. You can create either a normal User profile, or a restricted profile.
You'll now see a list of apps installed on your device,

with on/off toggles to the side. By default, the restricted prof access any of these. Go through the list and toggle on only th comfortable with your child accessing. The list includes any web browsers installed on your tablet, so leave these switched to off if you're worried about what harm your child may come to online. You can also click on the Settings icon next to Settings to allow apps to use location information, which is switched off by default.

Google Play Store Settings

Restrict 'in-app purchases

Protecting your 'wallet' is simple: open the Google Play Store app on your Android phone or tablet, then open the Settings menu and scroll down to User controls. Tick the box next to Password, which will request your Google account password whenever someone tries to download a paid app or purchase in-app extras.

Content Filtering

There is an option to set up Content filtering. Within this you can allow all apps, or only those rated as low, medium or high maturity, or for everyone. Tick the appropriate boxes and click Ok. Note that you'll need to create a password to stop a tech-savvy child from altering this setting.

Prevent your child from sharing their location

Location services allow applications such as maps and social networks to pinpoint your location.
You can disable Location services on iPads by going to the parental controls and selecting Off for Location.
You can disable location services for Facebook but allow your location to be used in Maps so you can find out where you are. Have a look through the different options and decide what is appropriate for your child. By then selecting Don't allow changes this locks the app-specific settings you have chosen and would prevent any new apps from using location services.