DURHAM LANE
PRIMARY SCHOOL
"Where children and families come first"

E-safety / Acceptable Use Policy

Reviewed: May 2020 (Andrew Beane)
Next Review due: May 2022

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment. Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites;
- Email and Instant Messaging;
- Chat Rooms and Social Networking;
- Blogs;
- Podcasting;
- Video Broadcasting;
- Music Downloading;
- Gaming;
- Mobile/ Smart phones with text, video and/ or web functionality;
- Other mobile devices with web functionality.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web based resources, are not consistently monitored. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Durham Lane Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Some of the dangers children 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;
- Cyberbullying;
- 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;
- Exposure to material on social media and the internet that could potentially draw children and their parents or carers towards supporting terrorism or becoming terrorists.

As with all other risks, it is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build pupils' awareness and 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 appropriately. Durham Lane Primary School will aim to educate its pupils in safeguarding themselves; equipping children with the skills they need to ensure that they can do everything that is reasonably expected of them, to manage and reduce these risks.

This E-Safety policy aims to highlight how we intend to educate and protect our pupils, 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.

This Policy should be read in conjunction with the following school policies:

- Safeguarding Policy;
- Health and Safety Policy;
- Whole School Behaviour Policy.

'Schools are finding that a blocking and banning approach, which merely limits exposure to risk, may no longer be a sustainable approach... Schools need to focus on a model of empowerment; equipping children with the skills and knowledge they need to use technology safely and responsibly, and managing the risks'

Becta Safeguarding Children Online Feb 2009

Whole School Approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-safety education programme for pupils, staff and parents.

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head Teacher, with the support of the Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-safety co-ordinator in our school from May 2015 is Andrew Beane.

All members of the school community have been made aware of who holds this post. It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as Stockton LEA, Northern Grid for Learning, DfE, CEOP (Child Exploitation and Online Protection), and Child Net. The e-safety co-ordinator ensures the Head teacher, Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- Safe use of e-mail;
- Safe use of the Internet;
- GDPR regulations
- Safe use of the school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of pupil information/photographs on the school website and school's Twitter account;
- Procedures in the event of misuse of technology by any member of the school community;
- Their role in providing e-safety education for pupils;
- Their role in ensuring that children are not exposed to material on social media and the internet that could potentially draw them towards supporting terrorism or becoming terrorists.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction. Supply Teachers must sign an acceptable use of ICT agreement before using technology equipment in school (see Appendix 1 for staff acceptable use

agreement). There is a procedure for the ICT co-ordinator and technician to follow when a member of staff leaves the school

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety posters will be prominently displayed.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety. E-safety will be taught under the guidance in the 2014 computing curriculum. (See Appendix 2 for pupil acceptable use agreement).

- We provide opportunities within a range of curriculum areas to teach about e- safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities as part of the computing curriculum.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (see section on Cyberbullying).
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the computing curriculum.

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- Our internet access is controlled through One IT's web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.
- Our web filtering service ensures that children are not exposed to images or media that could potentially draw them towards supporting terrorists or terrorism.

E-mail

The use of email within school is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. When appropriate, teachers may allow pupils to write emails using a class account. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or externally. We recognise that pupils need to understand how to style an email in relation to their age. The 2014 National Curriculum states use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

- Pupils are introduced to email as part of the new Computing National Curriculum.
- The school gives staff their own email account. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact pupils or parents using personal email addresses.
- Pupils may only use school approved accounts on the school system.
- The forwarding of chain letters is not permitted in school.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- All pupils must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone.
- Staff must inform (the e-safety co-ordinator) if they receive an offensive e- mail.

Use of digital and video images.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, pupils and parents/carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images can remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

The school will inform and educate users about these risks and will teach pupils, as appropriate, to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; **the personal equipment, including cameras and mobile phones, of staff should not be used for such purposes**.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute, e.g. swimming.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website or school's Twitter account, or elsewhere that includes pupils, will be selected carefully and will comply with good practice guidance on the use of such images.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or Twitter account (signed by parents or carers at the start of the pupil's school career).

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Managing social networking, social media and personal publishing sites

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content.

Although primary age pupils should not use Facebook, Instagram, Twitter, Snapchat or similar sites, pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning pupils' underage use of sites.
- No member of staff should use social networking sites or personal publishing sites to communicate with students, past or present.
- Staff need to be aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.
- Teachers cannot under any circumstances mention any references to their working lives on any social media.
- Staff personal use of social networking, social media and personal publishing sites guidelines will be issued as part of staff induction and outlined in the school Staff Acceptable Use Policy
- A sample advice leaflet for parents on Social Networking Sites, in particular, Facebook, should be issued to parents when and where appropriate

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by two members of staff when video conferencing
- Approval from the Head Teacher is sought prior to all video conferences within school.
- See Appendix 8 for the school's video conferencing protocol.

Managing Mobile Phones and Personal Devices

- The use of mobile phones and other personal devices by pupils and staff in school is outlined in the Staff Handbook and covered in the School Acceptable Use policy, and includes:
- All mobile phones must be switched off during directed time and should not be used in the presence of children. Personal mobile phones should NEVER be used to take photographs.
- Mobile phones and personal devices **are not** permitted to be used in certain areas within the school site such as the children's toilets.
- All visitors will be told to switch off their mobile phones on entering the building. There are signs in the main entrance and in the Nursery entrance reminding visitors of this.

Pupils' use of personal devices:

If a pupil brings a mobile device to school then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers at the end of the school day.

Staff use of personal devices:

- Staff **are not** permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- As outlined in the Staff Handbook, mobile phones and devices must be switched off during teaching periods and such devices should be stored securely during this time away from children.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Password Security

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. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Follow password guidelines ('Password Protocol 2006', Northern Grid, in Appendix 3).
- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety rules.
- Users are provided with an individual network username. Children are expected to use a personal password to access their account and keep it private.
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a password may have been compromised or someone else has become aware of the password the child or adult must report this to the e-safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.

Levels of security for data. Taken from 'Safeguarding Tools Document' from National Education Network.

Restricted	Protect	Public
Personal information related to pupils or staff (usually contained in the Management Information System).	School routines, schedules and management information.	Website and promotional materials. Display material around school.

General Data Protection Regulation (GDPR)

Personal information about children is stored on our computer system and in paper records to help us with their educational needs. The Head Teacher is responsible for their accuracy and safe-keeping. School staff have access to children's records to enable them to do their jobs. From time to time information may be shared with others involved in children's, if it is necessary. Anyone with access to children's records has received training in the new GDPR regulations and is governed by a legal duty to keep their details secure, accurate and up to date. Data can only be accessed and used on school computers or laptops. Staff are aware they must not use their personal devices for accessing any school/ children/ pupil data.

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Stockton LEA can accept liability for material accessed, or any consequences of Internet access.

- Concerns relating to e-safety should be made to the e-safety co-ordinator. Any complaint about staff misuse must be referred to the Head teacher. Incidents should be logged and the Flowcharts for Managing an e-safety Incident should be followed (see Appendix 4).
- All users are aware of the procedures for reporting accidental access to inappropriate materials.
- The breach must be immediately reported to Durham Lane's e-safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/Stockton LEA, LADO, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart in Appendix 5).
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyber bullying

Cyber bullying is the use of computer technology, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site'. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber bullying. Here are some of the more common:

1. Text messages —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology);
2. Picture/video-clips via mobile phone cameras or social media - images sent to others to make the victim feel threatened or embarrassed, such as Instagram or Facebook;
3. Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible;
4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name;
5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatroom, such as Skype;
6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using MSM (Microsoft Messenger), Yahoo Chat or Facebook;
7. Bullying via websites — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo and MySpace.

The best way to deal with cyber bullying is to prevent it happening in the first place and to have clear steps to take when responding to it.

Preventing cyber bullying

It is important that we work in partnership with pupils and parents to educate them about cyber bullying as part of our e-safety curriculum.
They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them;
- know what to do if they or someone they know are being cyber bullied;
- report any problems with cyber bullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet.

Additional online advice on how to react to Cyberbullying can be found on www.kidscape.org and www.wiredsafety.org

See Appendix 6 for Key Safety Advice for children, parents and carers

Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts,
- changing contact details.
- Take action to contain the incident when content has been circulated.
- Use disciplinary powers to confiscate phones that are being used to cyber bully.
- Ask the pupil who they have sent messages to in case of illegal content

Examples of illegal activity may include:

- child sexual abuse images;
- adult material;
- criminally racist material;
- other criminal conduct, activity or materials.

See Appendix 5 managing an e-safety incident involving illegal activity.

Investigating Incidents

All bullying incidents should be recorded and investigated in the Durham Lane Primary School e-safety incident log (see Appendix 9). We will:

- Advise pupils and staff to try and keep a record of the bullying as evidence;
- Take steps to identify the bully, including looking at the schools systems, identifying and interviewing possible witnesses, and contacting the service provider and police if necessary.
  The police will need to be involved to enable the service provider to look into the data of another user.

Working with the bully and sanctions

Once the bully is identified, steps should be taken to change their attitude and behaviour by educating them about the effects of Cyberbullying on others. Technology specific sanctions for pupil engaged in Cyberbullying behaviour could include limiting or refusing internet access for a period of time or removing the right to bring a mobile into school. Factors to consider when determining the appropriate sanctions include:

- The impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of material?
- The motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

Communications Policy

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms and discussed with pupils at the start of each year
- Pupils will be informed that network and Internet use will be monitored.
- E-safety will be included more prominently in both the PSHE and Computing curriculum.

Introducing staff to the e-safety policy

- All staff will be given the e-safety policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on our e-safety policy will be provided as required.
- Teaching staff will be directed to be mindful of the teacher standards for professional conduct

Enlisting parents' support

At Durham Lane, we believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to computing and associated risks.

The school disseminates information to parents relating to e-safety where appropriate in the form of

- Information and celebration evenings
- Posters
- Website postings
- Newsletter items

Parents/carers are asked to read through and sign acceptable use of computing agreements on behalf of their child on admission to school. Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website and Twitter). A partnership approach with parents will be encouraged. This includes parents' evenings with suggestions for safe home Internet use. Advice on filtering systems and educational activities that include safe use of the Internet will be made available to parents.

Equal Opportunities - Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children.

Reviewing this Policy

This policy will be reviewed, along with the Acceptable Use Policy, on a two-yearly basis. It will encompass new technologies and developments. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. Staff, governors, parents and children (via our Durham Lane School Council) will be consulted on any changes.

Appendix 1: Staff acceptable use of ICT agreement

DURHAM LANE PRIMARY SCHOOL

Acceptable Use of ICT Agreement Staff, Governor and Visitor 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 policy 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 Andrew Beane, school e-safety coordinator.

- I will switch off my mobile phone during directed time and not use it in the presence of children. Personal mobile phones will NEVER be used to take photographs in school.
- All visitors will be told to switch off their mobile phones on entering the building.
- 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 children and adults in school are not exposed to media that may potentially draw them towards supporting terrorists or terrorism. I will report any such activity to the e-safety coordinator and head teacher immediately,
- 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 personal data (such as data held on SIMS) 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 use or install any hardware or software without permission from the e-safety co-ordinators.
- 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 Head teacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request by the Head teacher.
- I will respect copyright and intellectual property rights.
- 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 e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

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)

Job title: .....

Appendix 2: Pupil acceptable use of ICT agreement

DURHAM LANE PRIMARY SCHOOL

Primary Pupil Acceptable Use of ICT Agreement/eSafety Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will not bring software, CDs or ICT equipment into school without permission.
- I will only use the Internet after being given permission from a teacher.
- 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 upsetting or not allowed at school. If I accidentally find anything like this, I will minimise the screen and tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- I will not use technology in school time to arrange to meet someone unless this is part of a school project approved by a 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 know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my eSafety.

Appendix 2: Pupil acceptable use of ICT agreement (Continued)

Dear Parents/Carers,

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in schools. We expect all children to be safe and responsible when using any ICT. Please read and discuss with your child the eSafety rules overleaf and return this sheet signed by both you and your child. If you have any concerns or would like some explanation please contact your child's class teacher.

This Acceptable Use of ICT Agreement is a summary of our eSafety Policy which is available in full, via our publications scheme, on request at the office or can be viewed on our school website.

Yours sincerely,

Mr A Beane

eSafety coordinator

Pupil:

I have read, understood and agreed with the Rules for Acceptable use of ICT (overleaf)

Signed ..... (child)

Parent's/Carer's Consent for Internet Access

I have read and understood the school rules for Acceptable Use of ICT and give permission for my son / daughter to access the Internet in school. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet.
I agree that should my son/daughter need to access the internet at home or anywhere else, that I will take all reasonable precautions to ensure he/she cannot access inappropriate materials and that he/she will use the computer in an appropriate manner.

Signed..... (parent/carer) Date.....

Appendix 3: Password Protocol (Northern Grid for Learning, 2006)

Passwords Protocol

Passwords are crucial to the security of your PC, Network and individuals. Never share your password with anyone even if you trust that person. Never provide a password if requested by email, this will likely be a fraudulent request.

In the event of inappropriate material being accessed or found on your PC or an IP the user can be traced by the logon and password used. If you have a shared password or have left your PC open via your password or shared your password with another user of friend you could be under suspicion.

All passwords should be complex in nature including capitals, lowercase, symbols and numerals. The more complex the password the more protection you are providing. Most people can remember a password of between 8-10 characters using single letters. However the more complicated the password, mixture of letter, numbers and symbols, the harder it is to remember.
A phrase password, which includes spaces, may be easier to remember. Try a phrase that is means something to you such as a line from a song or rhyme and try using it. If your system allows spaces this will add extra security.

If a single word is used and that word is in the dictionary, it is not safe. Hackers can run a programme that looks at all the words in a dictionary. This is called a "dictionary attack". The less variation in your password, the longer it should be. If you are only using letters it needs to be much longer than a password composed of, letters, symbols and numerals.

Make sure your password isn't related to you e.g. your name.
Numeric sequences such as 12345, 54321, 01010, 666666,999999999 etc. should not be used, as these are very easy for someone to guess if they are trying to gain access to your computer.
Look alike letters used in a simple word are not secure, e.g. "a" replaced with @, "s" replaced with $ - to a hacker this type of password is very basic. Look a likes are okay if used as part of a mixed symbol password such as:

Example: R@!Rt"M£B – rated as a strong password.
This is made from the rhyme **R**ound **a**nd **R**ound **t**he **M**ulberry **B**ush with symbols added between the letters.
However by adding spaces as well as symbols a simple password can be made very strong without making it difficult to remember e.g. R! a! R! t! M! B! (each letter has an exclamation mark and a space.)

If your system does not allow spaces add in an extra symbol instead e.g. R!"a!"R!"t!"M!"B!" If you write down your password make sure it is kept safe and not stored next to your PC. Once you have chosen and remembered your password do not be tempted to use it for all systems on your computer. If one password is compromised your whole system will then be open to abuse. You need to use multiple passwords of equal complexity.

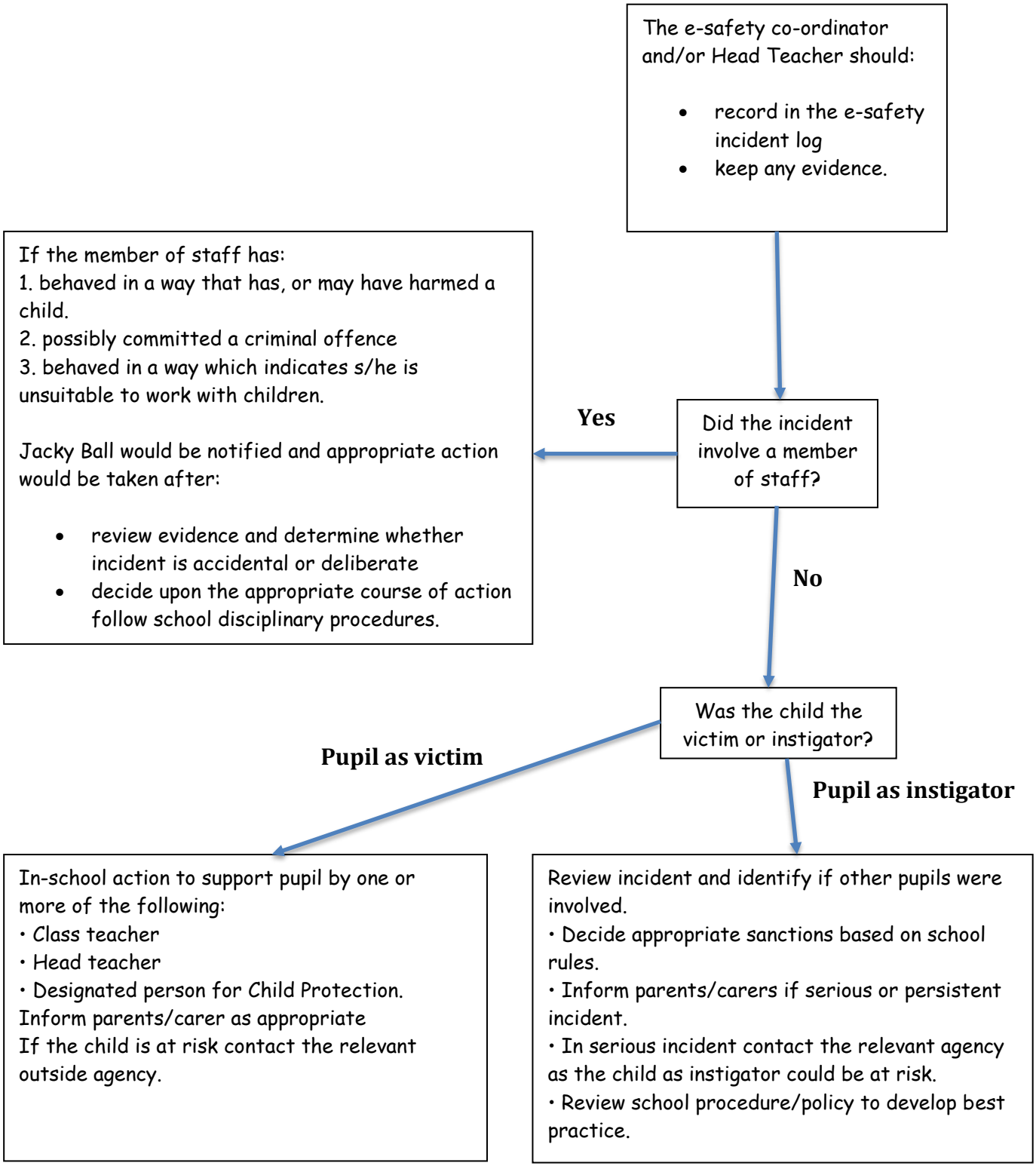
To test how secure your password is go to:

www.microsoft.com/athome/security/privacy/password_checker.mspx
This page on the Microsoft website offers you the opportunity to test whether your password is sufficiently complex to provide the security you need. You can also keep trying out passwords until you compose one that is secure.

Appendix 4: Managing an e-safety incident not involving any illegal activity

Incidents not involving any illegal activity, such as:

- using another person's user name and password
- accessing websites which are against school policy
- using a mobile phone to take video during a lesson
- using the technology to upset or bully (in extreme cases this could be illegal.)

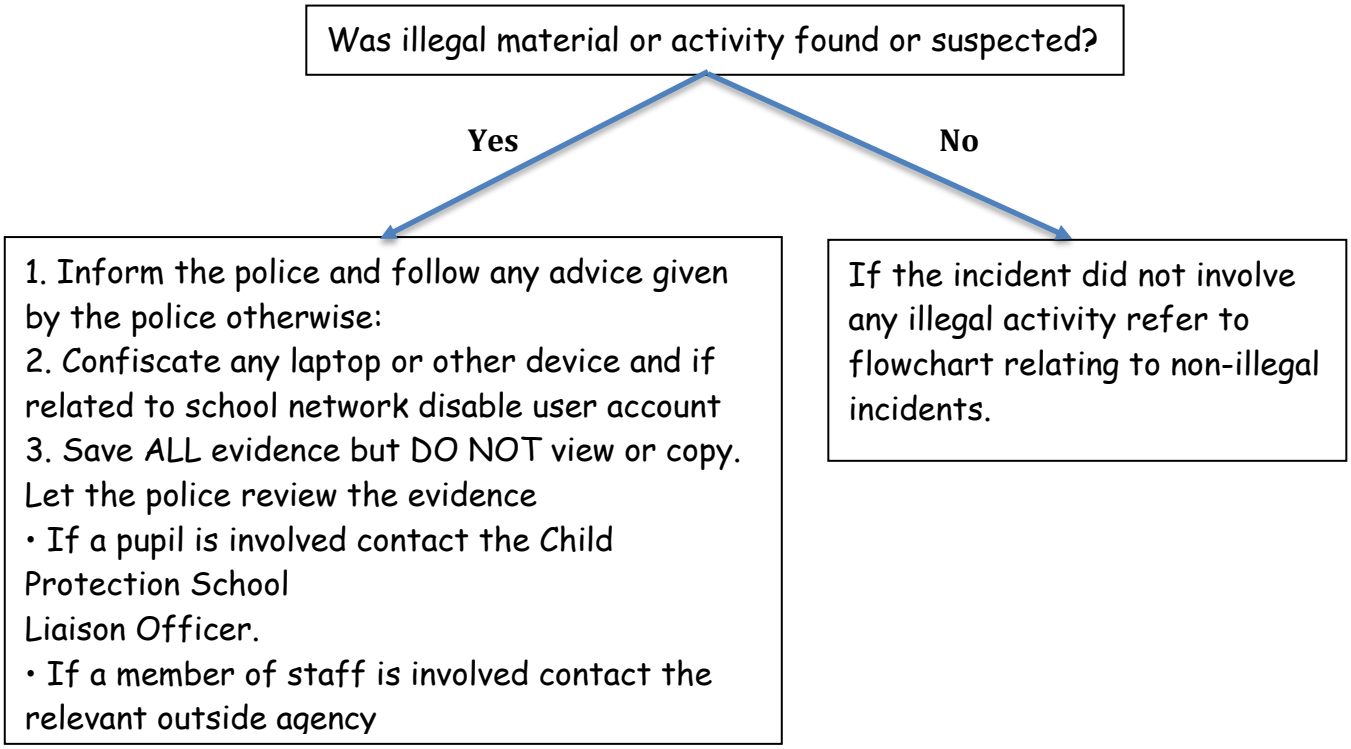


Appendix 5: Managing an e-safety incident involving any illegal activity

Illegal means something against the law, such as:

- downloading child pornography
- passing onto others images or video containing child pornography
- inciting racial or religious hatred
- promoting illegal acts

Following an incident the e-safety co-ordinator and/or Head Teacher will need to decide quickly if the incident involves any illegal activity.



<u>Appendix 6:</u> Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

- Remember, bullying is never your fault. It can be stopped and it can usually be traced.
- Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.
- Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.
- Don't give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.
- Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.
- If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyberbullying. For example,
www.kidscape.org and **www.wiredsafety.org** have some useful tips:

Text/video messaging
You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit **www.wiredsafety.org**.

If the bullying persists, you can change your phone number. Ask your mobile service provider.
Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.
Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.
Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls
If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off. Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.

Don't give out personal details such as your phone number to just anyone. Never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not. You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.

Don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again. Almost all calls nowadays can be traced.

If the problem continues, think about changing your phone number. If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails
- Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.
- Keep the emails as evidence. And tell an adult about them.
- Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. **abuse@hotmail.com**

- Never reply to someone you don't know, even if there's an option to 'unsubscribe'.
- Replying simply confirms your email address as a real one.

Web bullying
If the bullying is on a website (e.g. Bebo) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don't actually know the bully's identity. Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging
- Never give out your name, address, phone number, school name or password online.
- It's a good idea to use a nickname. And don't give out photos of yourself.
- Don't accept emails or open files from people you don't know.
- Remember it might not just be people your own age in a chat room.
- Stick to public areas in chat rooms and get out if you feel uncomfortable.
- Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.
- Think carefully about what you write; don't leave yourself open to bullying.
- Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way
- Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.
- If someone insults you online or by phone, stay calm – and ignore them.
- Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else.

Appendix 7: E-Safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the e-safety coordinator. This incident log will be monitored termly by the e-safety co-ordinator and Head teacher.

Date and time	Name of pupil or staff member	Male or female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Appendix 8: Video Conferencing Protocol

Using 'Zoom' online with a class of children

The following protocol will be followed when using 'zoom' to connect with classes of children.

The following terms are used:
Host = teacher/s controlling the session
Participant = child attending the session
Meeting = the online session
Meeting room = participants wait here to be admitted into the 'meeting'

Risk	Avoidance
Parental consent	A parent / responsible adult to be present once their child has been admitted from the meeting room and seen by teacher on video link to confirm consent. Parent does not have to remain in the video for the rest of the meeting.
Inappropriate content in the online chat.	Non-host adult to monitor the chat. Children reminded of rules for chat online.
Unknowns joining the group	Participants held in the meeting room and allowed one by one to be verified by host.
Participants speaking over each other	All participants muted on entry. Participants to put hands up to speak then host unmutes. Host to mute all participants and untick the blue box so that participants cannot unmute themselves
Inappropriate content being discussed	All participants reminded of usual classroom rules before session begins.
Children annotating the screen during screen sharing	If it happens, children told not to annotate the screen during screen sharing. If it does not happen, do not mention it as they probably do not know it can be done. Host can delete all annotations.
Participants wearing inappropriate clothing / displaying inappropriate content in background of video link.	Rules regarding clothing being appropriate for school explained before session begins. Children reminded that inappropriate content should not be in the background of their image on the video link.
Safeguarding adult hosts	At least two members of school staff to participate in zoom 'meetings' so that one adult is not alone with the group.