GREENHAUGH PRIMARY SCHOOL

On-line Safety & COMPUTER ACCEPTABLE USE POLICY

1. INTRODUCTION & OVERVIEW

At Greenhaugh Primary School, we are committed to ensuring that pupils are provided with the skills they will need in an expanding world of technology. We recognise the importance of online learning in developing children's knowledge and understanding of the world around them and consider Computing as an essential part of our curriculum.

With the continuing use of ICT in school, comes a responsibility to provide children with a safe environment to extend and explore their technological understanding.

As in other areas of life, children are vulnerable and could expose themselves to danger, whether knowingly or unknowingly, when using the internet and other technologies. Furthermore, some young people may find themselves involved in activities which are inappropriate, or possibly illegal.

This policy outlines our expectations of pupils, staff, parents, governors and members of the wider community to ensure best practice in helping children to be safe online.

1.1 Aims

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Greenhaugh Primary School with respect to the use of ICT-based technologies;
- safeguard and protect the children and staff of Greenhaugh Primary School;
- assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice;
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use;
- have clear structures to deal with online abuse such as cyber bullying which is cross referenced in our Anti-bullying policy;
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken;
- minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

1.2 The main areas of risk for our school community can be summarised as follows (the three C's):

Content:

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse;
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites;
- hate sites;

- content validation: how to check authenticity and accuracy of online content.

Contact:
- grooming;
- cyber-bullying in all forms;
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords.

Conduct:
- privacy issues, including disclosure of personal information;
- digital footprint and online reputation;
- health and well-being (amount of time spent online (internet or gaming));
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images);
- copyright (little care or consideration for intellectual property and ownership – such as music and film).

1.3 Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- policy to be posted on the school website /given to staff;
- policy to be part of school induction pack for new staff;
- online safety rules and acceptable use agreements issued to pupils and parents and signed at the start of each year;
- signed online safety rules and computer acceptable use agreements from children and parents to be held in admin office;
- online safety rules and computer acceptable use agreements issued to staff and signed accordingly. Copies held in Safeguarding Central Register (SCR).
- Parents made aware of the School's Filtering and Monitoring Systems

1.4 Handling complaints:

The school will take all reasonable precautions to ensure online 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 the Local Authority can accept liability for material accessed, or any consequences of internet access.

When handling a complaint, staff and pupils will be given information about possible sanctions as below.

Sanctions include:
- discussion between Online safety Co-ordinator / Headteacher and child or member of staff involved; informing parents or carers;
- removal of internet or computer access for a period of time;
- the Online safety Co-ordinator acts as first point of contact for any complaint which will be reported to the Headteacher;
- complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy;
- complaints related to child protection are dealt with in accordance with school / LA Safeguarding and Child Protection procedures;
- referral to LA / Police.

1.5 Review and Monitoring:

- the school has an Online safety Co-ordinator who will be responsible for review and updates;
- the online safety policy will be reviewed annually or more frequently if any significant changes occur with regard to the technologies in use within the school;
- the online safety policy has been written by the school Online safety Co-ordinator and is current and appropriate

for its intended audience and purpose;
- the policy is circulated to staff and governors and is available on the website and has been approved by the Governing Body;
- all amendments to the school e- safety policy will be discussed in detail with all members of teaching staff.
- The Online Safety Co-ordinator will complete the Northumberland Online Safety Audit tool annually.
- School devices and school filtering and monitoring services will be tested annually by the Online Safety Co-ordinator.
- In addition to annual checks systems and processes will be updated as needed.
-

2. EDUCATION & CURRICULUM

2.1 Pupil Online safety curriculum:

This school has a clear, progressive Online safety education programme as part of the Computing curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:

- to STOP and THINK before they CLICK
- to develop a range of strategies to evaluate and verify information before accepting its accuracy;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand acceptable behaviour when using an online environment i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;
- [for older pupils] to understand why and how some people will 'groom' young people;
- to understand the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying;
- to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP (Child Exploitation & Online Protection) button;
- plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- ensure staff will model safe and responsible behaviour in their own use of technology during lessons;
- ensure that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- ensure that staff and pupils understand the issues around aspects of the commercial use of the internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling.

2.2 Staff and governor training:

This school

- will continue to train staff and governors on online safety issues and the school's online safety education;
- provide, as part of the induction process, all new staff with information and guidance on the Online safety & Computer Acceptable Use Policy.

2.3 Parent awareness and training:

This school raises awareness to parents by:

- ensuring that the Online safety & Computer Acceptable Use Agreements to parents and pupils are renewed annually where the principles of online safety behaviour are made clear;
- information leaflets; in school newsletters; on the school web site;
- demonstrations, practical sessions may be held at school;
- suggestions for safe internet use at home;
- provision of information about national support sites for parents;
- Information on the School's Filtering and Monitoring Systems will be shared with parents annually.

3. EXPECTED CONDUCT & INCIDENT MANAGEMENT

3.1 Expected conduct:

In this school, all users:

- are responsible for using the school Computing systems in accordance with the relevant Online safety Rules & Computer Acceptable Use Policy which they will be expected to sign before being given access to school systems;
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety & Computer Acceptable Use Policy covers their actions out of school, if related to their membership of the school i.e. through social media;
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images, cyber-bullying and the use of social media.

Staff:

- are responsible for reading the school's Online safety & Computer Acceptable Use Policy and using the school ICT systems accordingly, including the use of mobile phones, hand held devices and social media;
- understand that sanctions will result from misuse.
- Discuss risks without attaching blame or shaming children, so that they feel bale to share concerns or worries with staff.

Pupils:

- use ICT equipment appropriately respecting online safety behaviour guidelines taught in school;
- Know who to go to if they are concerned about something they have seen online.
- understand that sanctions will result from deliberate misuse.

Parents/Carers:

- should provide consent for pupils to use the internet, as well as other technologies, as part of the online safety acceptable use agreement form at time of their child's entry to the school;
- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.

3.2 Incident Management:

In this school:

- there is strict monitoring and application of the Online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions ;
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- support is actively sought from other agencies as needed (e.g. the Local Authority, UK Safer Internet Centre helpline) in dealing with online safety issues;
- SENSO is sued to monitor students and staff's online activity and reports any breaches.
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school;
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible;
- we will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

4. MANAGING THE ICT SYSTEMS

4.1 Filtering and Monitoring

Internet access, security (virus protection) and filtering:

This school:

- has the educational filtered secure broadband connectivity through NCC (Northumberland County Council). Fortinet blocks illegal and inappropriate content.
- ensures the system is healthy through use of Panda Security anti-virus software ;
- uses secured email to send personal data over the Internet and uses encrypted devices or secure remote access where staff need to access personal data off-site;
- works in partnership with NCC to ensure any concerns about the system are communicated so that systems remain robust and protect pupils and staff;
- is vigilant in its supervision of pupils' use at all times, as far as is reasonable;
- ensures all staff and pupils have signed an Online safety Rules and Acceptable Use agreement form and understand that they must report any concerns;
- requires staff to preview websites before use;
- plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines;
- is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- informs all users that internet use is monitored;
- informs staff and students that that they must report any failure of the filtering systems directly to the Online safety Co-ordinator who then takes the appropriate action;
- makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA (Local Authority).
- Uses SENSO, which sends weekly violation reports if a capture has been made.

4.2 Network management (user access, backup):

To ensure the network is used safely, this school:

- makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- ensures that pupils and staff (including supply teachers) have their own user name and password to access the internet. Staff and pupils are shown how to save work and access work from these areas if appropriate;
- requires all users to always log off when they have finished working or are leaving the computer unattended;

- where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves;
- requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day;
- has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- equipment that belongs to school does not go home with pupils;
- makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities;
- makes clear that staff accessing LA systems do so in accordance with any corporate policies; e.g. email or Intranet; finance system, personnel system etc;
- ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems;
- does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or MIS Support (SIMS);
- makes clear responsibilities for the back up of MIS and finance systems and other important files;
- has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data;
- uses the DfE (Department for Education) secure S2S (School to school) website for all CTF files (common transfer files) sent to other schools;
- ensures that all pupil level data or personal data sent over the internet is encrypted or only sent within the approved secure system ;
- follows NCC advice on security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- our wireless network has been secured;
- all computer equipment is installed professionally and meets health and safety standards;
- projectors are maintained.

SIMS (School Management Information System) is accessed through the admin system only and is password protected.

Data backup and disaster recovery plan:
The school has a disaster recovery plan which ensures continuity of service and security of data in the case of an emergency or other unforeseen event.

- the backup of data is performed every week or more frequently if a large amount of data has been updated;
- the backup is created on an external hard drive which is held in a locked container in the admin office;
- the admin member of staff is responsible for the backup and protection of data in accordance with GDPR.

4.3 Passwords policy:

This school makes it clear that staff and pupils must:
- always keep their password private;
- must not share it with others;
- must not leave it where others can find it.

All staff have their own unique username and private passwords to access school systems.

4.4 Email:

This school:
- provides relevant staff with an email account for their professional use, and makes it clear that personal email should be through a separate account;
- maintains that all emails must include a '**signature**' comprising of:

  Name, Job Title, School name, Contact telephone number
- ensures that staff have a duty of care to keep their email facility secure;

- reminds members of staff that it is their duty, **when using remote access**, to log off when finished and **that they must never leave any device unattended whilst still logged on**;
- prohibits the use of email for purposes which may be illegal, or the making or sending of email messages which may be considered to be offensive in any way;
- does not publish personal e-mail addresses of pupils or staff on the school website. For communication with the wider public the school admin address is published on the website;
- will contact the Police if one of our staff receives an e-mail that we consider is particularly disturbing or breaks the law;
- will ensure that email accounts are maintained and up to date;
- reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police;
- knows that spam, phishing and virus attachments can make e mails dangerous. We use the anti-virus product Sophos.

Staff:

- staff can access the LA email systems from anywhere, but only with their own username, password and validated information submitted from their personal identity grid document;
- The use of personal devices to access school email is governed within the Acceptable Use Policy Agreement. This includes taking personal responsibility for the physical security of the device and implicit instructions regarding the use of the device by other family members etc. that school systems are kept secure, closed down, logged out by the staff member.

- staff only use LA email systems for professional purposes;

- Re-affirmation of keeping personal data secure is made annually within the CAU agreement. Saving of attachments containing personal information is mandated to school equipment only;

- access in school to external personal email accounts may be blocked;
- never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer);
- staff know that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper;
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- embedding adverts is not allowed;
- all staff read and sign our Online safety Rules and Computer Acceptable Use Agreement document to say they have read and understood the online safety rules, including email and where it is explained how any inappropriate use will be dealt with.

4.5 School website:

- the Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- the school web site complies with the statutory DfE guidelines for publications;
- the point of contact on the website is the school address, telephone number and we use a general email contact address - admin@greenhaugh.northumberland.sch.uk. Personal information or individual email identities will not be published;
- photographs of children published on the website do not have names attached.

4.6 Social networking:

School staff will ensure that in private use:

- no reference should be made in social media to pupils, parents / carers or school staff;

- staff must not ‘friend’ a pupil or parent through social media;
- personal profiles are not linked to employment in a named school;
- they do not engage in online discussion on personal matters relating to members of the school community;
- personal opinions should not be attributed to the school or local authority.

Staff will ensure that
- The school’s Facebook page has a pinned post stating that the school will never name any child on the page and asking that no-one else does. If a child is named the post will be deleted (see School Facebook policy)
- The school will have written permission from a parent or carer to share any photo of their child on Facebook

5. DATA SECURITY: MANAGEMENT INFORMATION SYSTEM

System access and Data transfer:

5.1 Strategic and operational practices:

At this school:
- we have listed the IT equipment held in school on the Asset Register / Property Audit record. This is reviewed annually and updated accordingly;
- we ensure that any incidents where data protection may have been compromised are reported to the Headteacher;
- all staff are DBS (Disclosure & Barring Service) checked and records are held in one central record held in a locked cupboard and on the Admin system;
- we ensure ALL the school stakeholders sign an Online safety Rules & Computer Acceptable Use Agreement form. These are for **staff** , and for **pupils & parents** and are held in the admin office in school;
- we follow LA guidelines for the transfer of any data, such as MIS (Management Information System) data or reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services;
- school staff with access to setting-up usernames and passwords for email, network access are working within the approved system (currently provided through our NCC purchased IT Admin Service Level Agreement) and follow the security processes required by those systems;
- we ask staff to undertake regular house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

5.2 Technical Solutions:

- staff have secure area(s) on the system to store sensitive documents or photographs which are password protected;
- we require staff to log-out of systems when leaving their computer;
- we use an encrypted pen drive if any member of staff has to take any sensitive information off site;
- we use the DfE S2S site to securely transfer CTF pupil data files to other schools;
- any technical equipment taken ‘Off Site’ for educational purposes is logged out and then back into school in the ‘Off Site Property Resister’ stored in the admin office;
- we comply with the WEEE (Waste Electrical & Electronic Equipment) directive (see below) on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held and get a certificate of secure deletion for any server that once contained personal data;
- portable equipment loaned by the school (for use by staff at home), where used for any protected data, is disposed of through the same procedure.

Asset disposal:
Details of all school-owned hardware is recorded in a hardware inventory.
All redundant equipment is disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

6. EQUIPMENT & DIGITAL CONTENT

6.1 ipads:

- no credit card or other payment method should be assigned to the tablet;
- pupils are not allowed to download any App. In particular, no Social Media apps are to be downloaded. The content of each ipad is monitored;
- all ipads are configured to use the school Wi-Fi network where they are subject to filtering;
- use of the ipads for questionable activity including the deliberate viewing of inappropriate material via the internet is not permitted;
- when in a lesson, pupils should only engage with those apps that support their learning under the guidance of their teacher. Sanctions will apply for any learners using their ipads inappropriately during learning sessions;
- charging is the responsibility of the users and all ipads should be brought back to the charging unit at the end of the day.

6.2 Personal mobile phones and mobile devices:

- mobile phones brought into school are entirely at the staff's, parents' or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into school;
- staff members may only use their phones during break times which must be stored and used safely in the staffroom;
- the recording, taking and sharing of images, video and audio on any mobile phone or mobile device is not permitted on the school premises; except for parents/carers during school performances. Parents/ carers sign to say that they will not share any photos on any social media.
- the Headteacher reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material;
- mobile phones must not be used to communicate between staff and parents. The school landline must be used in all circumstances. The only exception to this rule is a nominated mobile phone on an off-site school visit for emergency purposes;
- no images or videos should be taken on mobile phones or personally-owned mobile devices;
- if a member of staff breaches the school policy then disciplinary action may be taken.

6.3 Pupils' use of personal devices:

- the School does not allow pupil mobile phones or devices in school;
- Smart watches that enable children to take photos or videos or to send or receive messages, calls or emails are not allowed in school.
- if a pupil breaches the school policy 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 or carers in accordance with the school policy.

6.4 Digital images and video:

In this school:

- we gain parental / guardian permission for use of digital photographs or video involving their child as part of the school agreement form in the Autumn term of each school year;
- we do not name pupils in online photographic materials;
- staff sign the school's Online safety Rules & Computer Acceptable Use Agreement and this includes a clause on the non-use of mobile phones / personal equipment for taking pictures of pupils;
- if specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school has already obtained individual parental permission for its use;
- pupils are taught that they should not post images or videos. We teach them about the risks associated with

providing information with images that reveal the identity of themselves or others and about their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Role	Key responsibilities
Headteacher Clare Crow **Headteacher**	● to take overall responsibility for online safety provision ● to take overall responsibility for data and data security ● to ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements, currently NCC ● to be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant ● to be aware of procedures to be followed in the event of a serious online safety incident. ● to receive regular monitoring reports from the online safety Co-ordinator ● to ensure that there is a system in place (PCE – Policy Central Enterprise) to monitor and support staff who carry out internal online safety procedures.
Online safety Co-ordinator and/or Designated Safeguarding Lead Clare Crow & Alice Johnston	● takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents ● promotes an awareness and commitment to online safety throughout the school community ● ensures that online safety education is embedded across the curriculum ● liaises with school ICT technician ● communicates regularly with the designated online safety Governor to discuss current issues, review incident logs and filtering ● ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident ● ensures that an online safety incident log is kept up to date ● facilitates training and advice for all staff ● liaises with the Local Authority and relevant agencies ● is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from: ▪ sharing of personal data ▪ access to illegal / inappropriate materials ▪ inappropriate on-line contact with adults / strangers ▪ potential or actual incidents of grooming ▪ cyber-bullying and use of social media ● to report any online safety related issues that arise, to the designated safeguarding lead ● to ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed ● to ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date ● to ensure the security of the school ICT system ● to ensure that access controls / encryption exists to protect personal and sensitive information held on school-owned devices

	● that the use of the network / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online safety Co-ordinator / Headteacher for investigation / action / sanction ● to ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
Online safety Governor Jenni Holland, Chair of Govs	● ensures that the school follows all current online safety advice to: ▪ keep the children and staff safe ▪ review the Online safety Policy and review the effectiveness of it ▪ support the school in encouraging parents and the wider community to become engaged in online safety activities. ● The role of the Online safety Governor will include: ▪ regular reviews with the Online safety Co-ordinator ▪ to oversee the delivery of the online safety element of the computing curriculum ▪ to liaise with the designated safeguarding lead (DSL) on online safety.
Office Manager	● to ensure that all data held about pupils on the school admin system has appropriate access controls in place.
Teachers	● to embed online safety issues in all aspects of the curriculum and other school activities ● to supervise and guide pupils carefully when engaged in learning activities involving online technology (including extra-curricular and extended school activities if relevant) ● to ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content, such as Copyright law.
All staff	● to read, understand and help promote the school's online safety policies and guidance ● to read, understand, sign and adhere to the staff Online safety Rules & Computer Acceptable Use Agreement (see Appendix 3) ● to be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they use and implement current school policies with regard to these devices ● to report any suspected misuse or problem to the Online safety Co-ordinator ● to maintain an awareness of current online safety issues and guidance e.g. through CPD (continuous professional development) ● to model safe, responsible and professional behaviours in their own use of technology ● to ensure that there is NO digital communication with pupils e.g. through social media, email, text or mobile phones etc
Pupils	● to read, understand, sign and adhere to the Pupil Online safety Rules & Computer Acceptable Use Agreement (see Appendix 2) ● to have a good understanding of research skills and the need to avoid plagiarism (copying directly) and uphold copyright regulations ● to recognise abuse, misuse or inappropriate materials ● to know what action to take if they, or someone they know, feels worried or vulnerable when using online technology ● to know and understand school policy on the use of mobile phones,

	digital cameras and hand held devices ● to know and understand school policy on the taking of images on digital devices and on cyber-bullying ● to take responsibility for learning about effective online safety practice when using online digital devices both in school and at home
Parents/Guardians	● to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the internet and the Online safety Rules ● to read, understand and promote the school Online safety Rules & Pupil Computer Acceptable Use Agreement with their children ● to consult with the school if they have any concerns about their children's use of technology.
External groups / visitors	● any external individual / organisation that has been given permission by the school will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

Signed: …… Clare Crow, Headteacher

Signed: …….. Jenni Holland, Chair of Governors

Date: …….

Appendix 1

GREENHAUGH PRIMARY SCHOOL

Re: Pupil Online safety Rules & Computer Acceptable Use Agreement

Date:

Dear Parent / Guardian,

Computing, 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 our Online safety Rules and Computer Acceptable Use Agreement. When you have helped your child/ren to read and understand this important agreement, please ask your child to sign it, then sign it yourself and return the document to school. These will be held in school as part of our Online safety protocol.

If you have any concerns or would like some explanation please contact your child's class teacher.

This Online safety Rules and Computer Acceptable Use Agreement is a summary of our Online safety Policy which is available in full on our website or as a paper copy available on request from our Office/Reception.

Yours sincerely,

Headteacher

Appendix 2

GREENHAUGH PRIMARY SCHOOL

Pupil Online safety Rules & Computer Acceptable Use Agreement

- I will only use ICT in school for school purposes.
- I will not tell other people my 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, take pictures or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will tell a teacher immediately.
- I will not give out my own details such as my name, phone number or home address.
- 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 online safety.
- I will tell my adult if anything I see makes me feel uncomfortable.
- I understand that there will be consequences for my actions if I break the rules.

Pupil Agreement

I have read, understood and agree with these Rules above.

Signed: ……. (Pupil) Date: ……..

Parent / Guardian Consent for Online safety & Computer Acceptable Use

I have read and understood Greenhaugh Primary School's rules for Online safety & Computer Acceptable Use and give permission for my child to safely access the Internet in school. I understand that the school will take all due care to ensure that pupils cannot access inappropriate materials. I will take all reasonable precautions to help my child/ren understand the importance of following the rules to keep them e-safe.

Signed……...…… (Parent / Guardian) Date……..

Appendix 3

Greenhaugh Primary School
Staff Online safety Rules & Computer Acceptable Use Agreement

Computing and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents.

- I will only use the school's email / Internet / Intranet and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- The use of personal devices to access school email is governed within this Acceptable Use Policy. This includes taking personal responsibility for the physical security of the device and following our implicit instructions regarding the use of the device by other family members etc.

- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.

- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email
- address, to pupils or parents.
- I will only use the approved, secure email system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. I understand that I am responsible for the physical security of the mobile device and its contents. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher.
- I will not use or install any hardware (including USB sticks) or software without permission from the online safety co-ordinator.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I understand that images of pupils and/ or staff will only be taken, stored and used for professional purposes on school devices (not on a personal mobile phone or similar device) in line with school policy and with written consent of the parent, guardian 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.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute. I will not link my employment establishment with my name on any social media site and understand that there are consequences of disciplinary action if a breach is made.
- I will support and promote the school's Online safety & Computer Acceptable Use 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.

Staff understand that sanctions will result from Online safety misuse. Failure to comply with the above agreement could lead to a range of sanctions e.g. loss of privileges, disciplinary action etc.

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 role

Appendix 4

Flowchart for managing an online 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 illegal)

The Online safety co-ordinator / Headteacher should:

record the incident in the online safety incident log
keep any evidence

Did the incident involve a member of staff

YES

If the member of staff has:

behaved in a way that has, or may have, harmed a child
possibly committed a criminal offence
behaved in a way which indicates s/he is unsuitable to work with children

The Headteacher would be notified and appropriate action would be taken after:

A review of the evidence and decision upon whether incident is accidental or deliberate
Decide upon the appropriate course of action

NO

Was the child the victim or instigator?

Pupil as instigator

Review incident and identify if other pupils were involved

Decide appropriate sanctions based on school rules

Inform parent/guardian if serious or persistent incident

In serious incident contact the relevant agency as the child as instigator could be the risk

Review school procedure/policy to develop best practice

Pupil as victim

In school action to support pupil by one or more of the following:

Class Teacher
Headteacher
Designated Safeguarding Lead

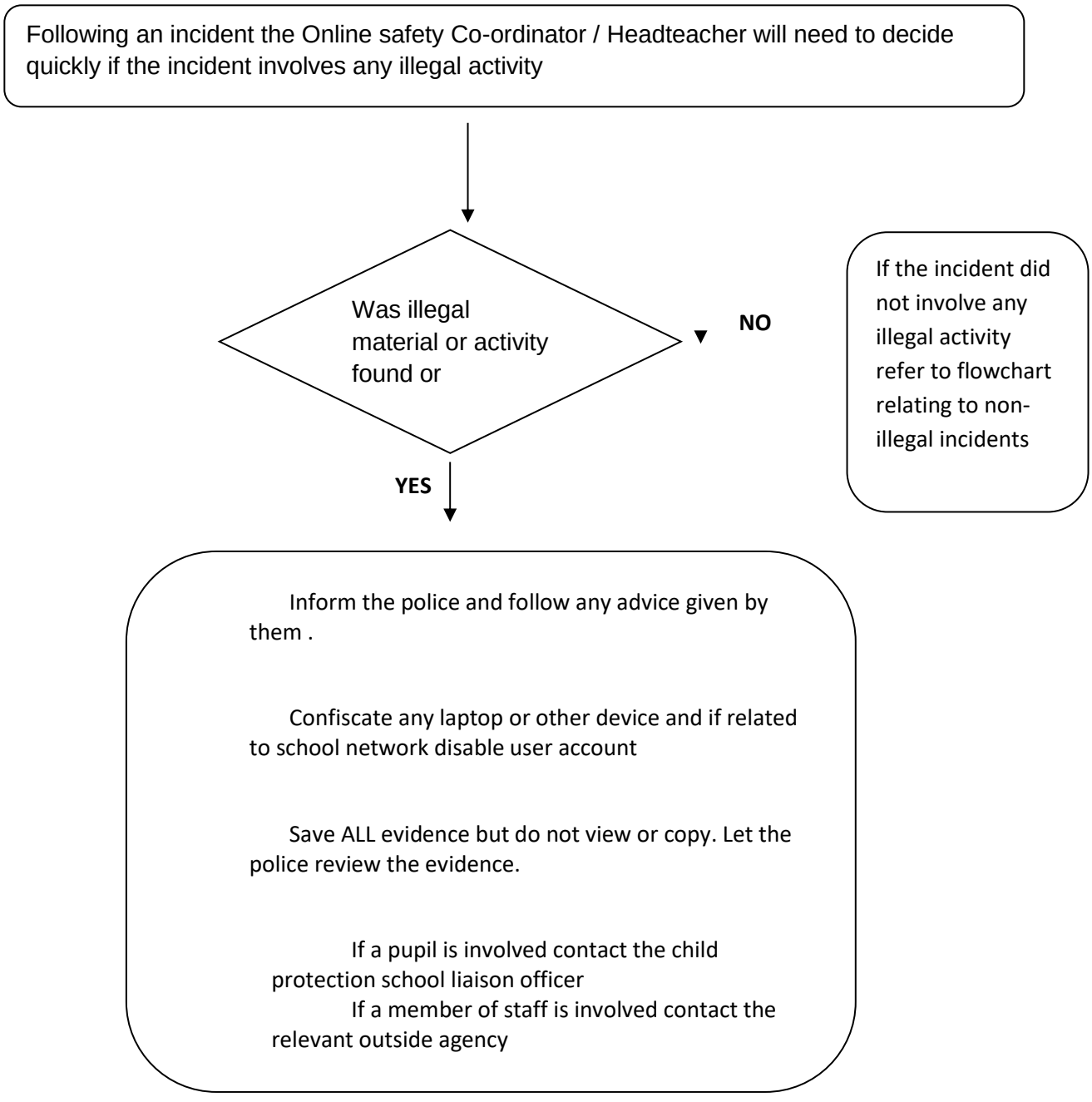
Inform parent / guardian as appropriate.

If the child is at risk contact the relevant outside agency

Flowchart for managing an online safety incident involving illegal activity

Illegal means something against the law, such as:

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



Reporting an online safety incident - all settings