Stubbins Primary School
Policy for e-Safety

At Stubbins School, children are at the centre of everything we do.
We aim to give our children the best possible opportunities and learning experiences, enabling them to reach their full potential. We aim to ensure that the children in our care are equipped for life-long learning as responsible citizens in an ever-changing, diverse local and world-wide community.
We believe that everyone has the capacity to become great if they have the courage to challenge themselves. By nurturing creativity, enjoyment & ambition; this policy supports our responsibility to make this happen.

Signed:	Signed: On behalf of the Governing Body
Head Teachers name: Mr A. J. Danson	Chair of Governors name: Mr. P. McKennell
Date: October 2020	Proposed Review date: October 2021

Contents

1. Introduction and Overview

Rationale
The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Stubbins Primary School with respect to the use of ICT-based technologies.
- safeguard and protect the children and staff of Stubbins 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 online bullying which are cross referenced with other school policies.
- 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 students.

The main areas of risk for our school community can be summarised as follows:
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/radicalisation/extremist/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- online-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)

(Ref Ofsted 2013)

Scope (from SWGfL)

This policy applies to all members of the Stubbins Primary School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school / academy ICT systems, both in and out of Stubbins Primary School.

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the *school* site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The *school* will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL • 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 / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures(e.g. network manager)

Online safety Co-ordinator / Designated Child Protection Lead	• 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-safeguarding throughout the school community
	• ensures that online-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated online- Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• To ensure 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
	  • online-bullying and use of social media

Governors / Online safety governor	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the online safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor • To 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 review with the online safety Co-ordinator / Officer (including online safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the online safety coordinator regularly

Role	Key Responsibilities
Network Manager/technician	• To report any e-Safety related issues that arises, to the online safety coordinator. • 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 exist to protect personal and sensitive information held on school-owned devices • the school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • that he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant • that the use of the *network / Virtual Learning Environment (LEARNING PLATFORM) / remote access / email* is regularly monitored in order that any misuse / attempted misuse can be reported to the *online safety Co-ordinator / Officer /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. • To keep up-to-date documentation of the school's e-security and technical procedures
LEARNING PLATFORM Leader	• To ensure that all data held on pupils on the LEARNING PLATFORM is adequately protected •
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
LGfL Nominated contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
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, extracurricular 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 laws
All staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Role	Key Responsibilities
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Policy (nb. at KS1 it would be expected that parents / carers would sign on behalf of the pupils) • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to 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 / use of images and on online bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's online safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home • to help the school in the creation/ review of online safety policies
Parent Liaison Officer	• Educating Parents and raising awareness as instructed by Head?
Parents/carers	• 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 school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website / LEARNING PLATFORM / on-line student / pupil records in accordance with the relevant school Acceptable Use Agreement. • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within school

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

- Policy to be posted on the school website and in the staffroom.
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure online safety behaviour. Due 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. However, it is an expectation that schools have procedures in place to address any issued that arise.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by tutor / Head of Year / online safety Coordinator / Headteacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA / Police.

- Our online safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher.

- Complaints of online bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

Review and Monitoring
The online safety policy is referenced from within other school policies: Computing policy, Child Protection policy, Anti-Bullying policy and in the School Development Plan, Behaviour policy, Personal, Social and Health Education and for Citizenship policies.

- The school has an online safety coordinator who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when 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 Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors and other stakeholders such as the PTA. All amendments to the school online safeguarding policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil online safety curriculum (digital literacy)

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on Safeguarding and online safety framework for EYFS to Y6/ national guidance. 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 / email, 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 for sexual reasons;
    - To understand the impact of online bullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including bullying; 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 button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures 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;
- Ensures 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;

Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff regarding online safety issues and the school's online safety education program; annual updates/ termly staff meetings etc.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safeguarding policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Acceptable Use Agreements to new parents, to ensure that principles of safe online behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to school systems. (At KS1 it would be expected that parents/carers would sign on behalf of the pupils.)
- 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 Policy covers their actions out of school, if related to their membership of the school
- 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 and online –bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand held devices.

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

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 and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues
- 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

Passwords policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find. ;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use strong passwords.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website. We use anonymous or group e-mail addresses, for example info@schoolname.la.sch.uk / head@schoolname.la.sch.uk / or class e-mail addresses (with one or more staff having access to an aliased/shared mailbox for a class) for communication with the wider public.
- Will contact the Police if one of our staff or pupils 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 a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product Sophos, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our internet access to the World Wide Web.

Staff:

- Staff can only use the LA or LGfL e mail systems on the school system
- Staff only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal e mail accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information ;
- 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); Collect; USO-FX*, named LA system;*
- Staff know that e-mail 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. That it should follow the school 'house-style':
    - 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 sign our LA / school Agreement Form AUP to say they have read and understood the e-safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. info@schooladdress or admin@schooladdress. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Social networking

Social networking sites (i.e. Facebook, Twitter. Instagram, Tumblr etc.) are becoming increasingly popular amongst the adult population and young people. However, many sites do have age restriction policies (ref: COPPA - Children's Online Privacy Protection Rule) where the minimum acceptable age is 13 years.
Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and anyone providing false information is violating the site 'Statements of rights'. For this reason, we would actively discourage pupils in our school using any social networking sites where these restrictions apply. Pupils who are found to be misusing websites where derogatory comments against other pupils, members of staff or the school are being made will have their internet access rights in school removed and in serious cases further action will be taken.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- 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 /academy* or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head Teacher is the Senior Information Risk Officer (SIRO).
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are. We have listed the information and information asset owners in a spreadsheet.
- We ensure staff know who to report any incidents where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record. We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form.
- We follow LA guidelines for the transfer of any data, such as MIS 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.
- We require that any Protect and Restricted material must be encrypted if the material is to be removed from the school and limit such data removal. / We have an approved remote access solution so staff can access sensitive and other data from home, without need to take data home.
- School staff with access to setting-up usernames and passwords for email, network access and Learning Platform access are working within the approved system and follow the security processes required by those systems.
- **STAFF SHOULD REFER TO THE SCHOOL DATA PROTECTION POLICY**
- **FOR SCHOOL DATA BREACH PROCEDURE SEE APPENDIX 9**

6. Equipment and Digital Content

All parents/carers are asked for their permission to allow the school to use digital images/photos of their child for use within school, in the school prospectus or on the school website/learning platform.
Our policy is to only use images where groups of children are involved in activities that represent the work pupils are doing, thus enabling the school to celebrate our achievements to others. To ensure our pupils' personal safety the school has a policy of not using full names of pupils to accompany images used.

In order to support this policy, we would ask parents/carers not to use any images of our pupils on social networking sites (i.e. Facebook). This includes any professional photos that have been purchased through the school and any photos taken during school concerts or sports events.

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's & parent's 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.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight until the end of the day. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School 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, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Where parents or students need to contact each other during the school day, they should do so only through the School's telephone. Staff may use their phones during break times. If a staff member is expecting a personal call they may leave their phone with the school office to answer on their behalf, or seek specific permissions to use their phone at other than their break times.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Mobile phones and personally-owned devices are not permitted to be used in certain areas within the school site, e.g. changing rooms and toilets.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- The Bluetooth or similar function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Personal mobile phones will only be used during lessons with permission from the teacher.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School strongly advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety.
- If a student 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.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- Students will be provided with school mobile phones to use in specific learning activities under the supervision of a member of staff. Such mobile phones will be set up so that only those features required for the activity will be enabled.
- **No pupil should have his or her mobile phone or personally-owned device with them in school. Any device brought into school must be handed in to the school office.**

Staff use of personal devices

- **The use of personal mobile phones is prohibited where children are present. All adults must keep their devices securely stored and out of sight where children are present.**
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students 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.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Digital images and video

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the 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 will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and 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.

Appendix 1: Image Consent Form

Parental Permission Form - use of photographs & digital images

Please sign and return to the school office

Dear Parents/Carers,

During your child's time at Stubbins Primary School, photographs & digital images may be taken of your son/daughter. These images may be used in a range of contexts:

- Training courses
- School publications, for example the prospectus
- Local newspapers as part of media coverage of a school event
- School website
- Display

Personal details of the children will **not** appear in any school publication or on the website. However, individual pupils' names may appear in a local newspaper, if appropriate to the article.

Please could you complete the permission slip below and return it to the school office as soon as possible.

If you do not want your son/daughter to appear in any photographs, please contact me.
Yours sincerely,

Mr. J. Danson

Headteacher

……

Parental Permission Form - use of photographs & digital images

I/We give permission for photographs of our son/daughter to be used by Stubbins Primary School.

Child's name	
Parent's signature	
Print name	
Date	

Appendix 2: Acceptable Use Policy – Staff & Visitors

ICT and the related technologies such as e-mail, the Internet and mobile devices are an integral part of our daily life in school. This agreement is designed to ensure that all staff and visitors are aware of their individual responsibilities when using technology. All staff members and visitors are expected to adhere to this policy and its contents at all times. Any concerns or clarification should be discussed with the Headteacher.

1. I will take responsibility for my own use of any technologies, making sure that I use them safely, responsibly and legally.

2. I will be an active participant in eSafety education, taking personal responsibility for my awareness of the opportunities and risks posed by the use of technology.

3. I will not use communications devices, whether school provided or personally owned, for bullying or harassment of others in any form.

4. I will not be involved with any online activities, either within or outside school that may bring the school, staff, pupils or wider members into disrepute. This includes derogatory/inflammatory comments made on Social Network Sites, Forums and Chat rooms.

5. I will not browse, download/upload or distribute any material that could be considered offensive, illegal or discriminatory.

6. I will respect copyright and intellectual property rights.

7. I will ensure that all electronic communications with pupils and other adults are appropriate.

8. I will not use the school system(s) for personal use during working hours.

9. I will not install any hardware or software without the prior permission of the Headteacher.

10. I will ensure that personal data (including data held on MIS systems) is kept secure at all times and is used appropriately in accordance with Data Protection legislation.

11. I will ensure that Images of pupils and/or adults will be taken, stored and used for professional purposes in line with school policy and with written consent of the parent/carer or relevant adult. I will not distribute images outside the school network without the prior permission of the parent/carer, or person/s in the image.

12. I will report any known misuses of technology, including the unacceptable behaviours of others.

13. I have a duty to respect the technical safeguards which are in place. I understand that attempting to breach technical safeguards or gain unauthorised access to systems and services is unacceptable.

14. I have a duty to report failings in technical safeguards which may become apparent when using the systems and services.

15. I have a duty to protect passwords and personal network logins, and should log off the network when leaving workstations unattended. I understand that any attempts to access, corrupt or destroy other users‟ data, or compromise the privacy of others in any way, using any technology, is unacceptable.

16. I understand that network activities and online communications are monitored, including any personal and private communications made using school systems.

17. I am aware that in certain circumstances where unacceptable use is suspected, enhanced monitoring and procedures may come into action, including the power to confiscate personal technologies such as mobile phones.

18. I will take responsibility for reading and upholding the standards laid out in the AUP. I will support and promote the school's eSafety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

19. I will abide by the school's rules for use of personal mobile equipment, including mobile phones, at all times.

20. I have read and understood the school's Digital Images & Video Policy and agree to abide by it

21. I understand that these rules are designed for the safety of all users and that if they are not followed, school sanctions will be applied and disciplinary action taken.

User Signature

I have read and agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature ……

Date ……

Full Name …… (PRINT)

Position/Role……

Appendix 3: Acceptable Use Policy – Pupils (Key Stage 1)

These rules are a reflection of the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring in equipment such as mobile phones, mobile games consoles or tablets etc. into school unless specifically asked to by my teacher.
- ✓ I will only go on online tools when a trusted adult is present.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or unkind.
- ✓ If I accidentally find anything that is inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will not tell other people online my name, phone number or address.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will only open or delete my own files.
- ✓ I know that these rules are to keep me safe.
- ✓ I know that my parents can be told if I break these rules.

……

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and …… [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at school.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class ……Date……

Appendix 4: Acceptable Use Policy – Pupils (Key Stage 2)

These rules are a reflection of the content of our school's eSafety Policy. It is important that parents/carers read and discuss the following statements with their child(ren), understanding and agreeing to follow the school rules on using ICT, including use of the Internet.

- ✓ I will only use ICT in school for school purposes.
- ✓ I will not bring in equipment such as mobile phones, mobile games consoles or tablets etc. into school unless specifically asked to by my teacher.
- ✓ I will only use the Internet and/or online tools when a trusted adult is present.
- ✓ I will only use my class e-mail address or my own school email address when emailing.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or nasty.
- ✓ I will not deliberately bring in inappropriate electronic materials from home.
- ✓ I will not deliberately look for, or access inappropriate websites.
- ✓ If I accidentally find anything inappropriate I will tell my teacher immediately.
- ✓ I will only communicate online with people a trusted adult has approved.
- ✓ I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- ✓ I will not give out my own, or others' details such as names, phone numbers or home addresses.
- ✓ I will not tell other people my ICT passwords.
- ✓ I will not arrange to meet anyone that I have met online.
- ✓ I will only open/delete my own files.
- ✓ I will not attempt to download or install anything on to the school network without permission.
- ✓ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ✓ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- ✓ I understand that failure to comply with this Acceptable Use Policy may result in disciplinary steps being taken in line with the school's Behaviour Policy.

……

Parent/ Carer Signature

We have discussed this Acceptable Use Policy and …… [Print child's name] agrees to follow the eSafety rules and to support the safe use of ICT at school.

Parent /Carer Name (Print) ……

Parent /Carer (Signature) ……

Class ……Date……

Appendix 5: Acceptable Use Policy – Parent's Letter

Stubbins Primary School
Learning and Growing Together

Dear Parent/Carer,

The use of ICT including the Internet, e-mail, learning platforms and today's mobile technologies are an integral element of learning in our school. To make this as successful and as beneficial as possible for all learners, we expect all pupils to act safely and responsibly when using technology both within, and outside of, the school environment.

This is particularly relevant when using Social Network Sites which are becoming increasingly popular amongst both the adult population and young people. However, many sites do have age-restriction policies where the minimum acceptable age is 13 years. Any child who sets up or uses such a site and is below the acceptable age is in clear breach of these age-restriction policies and therefore we actively discourage this in our school.

The enclosed ICT Acceptable Use Policy forms part of the wider School eSafety Policy and alongside the school's Behaviour Policy outlines those principles we expect our pupils to uphold for the benefit of both themselves and the wider school community.

Your support in achieving these aims is essential and I would therefore ask that you please read and discuss the enclosed ICT Acceptable Use Policy with your child and return the completed document as soon as possible.

Along with addressing eSafety as part of your child's learning, we will also be giving advice to parents and carers about eSafety during the school year. If you would like to find out more about eSafety for parents and carers, please visit the Lancsngfl eSafety website http://www.lancsngfl.ac.uk/esafety .

Signing the School Acceptable Use Policy helps us to maintain responsible use of ICT and safeguards the pupils in school. If you have any concerns or would like to discuss any aspect of the use of ICT in school, please do not hesitate to contact *me.*

Yours sincerely,

Mr. J. Danson
Headteacher

Stubbins Primary School
Bolton Road North,
Ramsbottom, Bury,
Lancashire. BL0 0NA

Tel: 01706 822063
www.stubbins.lancs.sch.uk

Headteacher: Mr A J Danson BEd, NPQH

Our KS1 Golden Rules for Staying Safe with ICT

✓We only use the Internet when a trusted adult is with us.

✓We only use the equipment that the teacher has given us permission to use.

✓We are always polite and friendly when using online tools.

✓We always make careful choices when we use the Internet.

✓We always ask a trusted adult if we need help using the Internet.

✓We always tell a trusted adult if we find something that upsets us.

Our KS2 Golden Rules for Staying Safe with ICT

- ✓ We always ask permission before using the internet or any ICT equipment.
- ✓ We only use the Internet when a trusted adult is around.
- ✓ We immediately close/minimise any page we are uncomfortable with (or if possible switch off the monitor).
- ✓ We always tell an adult if we see anything we are uncomfortable with.
- ✓ We only communicate online with people a trusted adult has approved.
- ✓ All our online communications are polite and friendly.
- ✓ We never give out our own, or others', personal information or passwords and are very careful with the information that we share online.
- ✓ We only use programmes and content which have been installed by the school.

Appendix 8:

Protocol for dealing with online safety incidents.

All incidents which are a cause for concern should be dealt with in exactly the same way as any other SAFEGUARDING concern, recorded and reported directly to the Headteacher or DSL.

Incident Log
All eSafety incidents must be recorded by the School eSafety Champion or DSL. This incident log will be monitored and reviewed regularly by the Headteacher and Chair of Governors. Any incidents involving Cyber bullying should also be recorded on the 'Integrated Bullying and Racist Incident Record Form 2' available via the Lancashire Schools" Portal.

Date & Time	Pupil(s) & staff Involved	Computer or System Involved	Incident Details	Action Taken

Appendix 9:

School Data Breach Procedure

Data Protection - Data Breach Procedure for Stubbins Primary School

Policy Statement

Stubbins Primary School holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by **Stubbins Primary School** and all school staff, Governors, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at **Stubbins Primary School** if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations
Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Types of Breach

A number of factors could cause data protection breaches. Examples are:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that the School identifies or is notified of a personal data breach, the following steps should followed:

1. The person who discovers/receives a report of a breach must inform the Head Teacher or, in their absence, either the Deputy Head Teacher and/or the School's Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.

2. The Head Teacher/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

3. The Head Teacher/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the school's responsibility to take the appropriate action and conduct any investigation.

4. The Head Teacher/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the School's legal support should be obtained.

5. The Head Teacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.

b. Contacting the relevant County Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all school staff. If staff receive an inappropriate enquiry, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual, making the enquiry, back. Whatever the outcome of the call, it should be reported immediately to the Head Teacher/DPO (or nominated representative).

c. Contacting the County Council's Communications Service, so that they can be prepared to handle any press enquiries. The Council's Media Relations can be contacted by telephone on **01772 534334**.

d. The use of back-ups to restore lost/damaged/stolen data.

e. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

f. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the Head Teacher/DPO (or nominated representative) to fully investigate the breach. The Head Teacher/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (pupils, staff members, suppliers etc.) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Head Teacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case-by-case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the School is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management Team and Full Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put this right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources or Internal Audit for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The Head Teacher/DPO should ensure that staff are aware of the School's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to the School's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the Head Teacher.

Appendix 10:

Protocol for dealing with online safety incidents.

Taken from the DfE publication: Searching, screening and confiscation Advice for Headteachers, school staff and governing bodies February 2014

Key points

Searching

- School staff can search a pupil for any item if the pupil agrees.
- Headteachers and staff authorised by them have a statutory power to search pupils or their possessions, without consent, where they have reasonable grounds for suspecting that the pupil may have a prohibited item.

  Prohibited items are:

  - knives or weapons
  - alcohol
  - illegal drugs
  - stolen items
  - tobacco and cigarette paper
  - fireworks
  - pornographic images
  - any article that the member of staff reasonably suspects has been, or is likely to be, used to commit an offence, or o to cause personal injury to, or damage to the property of, any person (including the pupil).
- Headteachers and authorised staff can also search for any item banned by the school rules which has been identified in the rules as an item which may be searched for.

Confiscation

- School staff can seize any prohibited item found as a result of a search. They can also seize any item, however found, which they consider harmful or detrimental to school discipline.

Schools' obligations under the European Convention on Human Rights (ECHR)

- Under article 8 of the European Convention on Human Rights pupils have a right to respect for their private life. In the context of these particular powers, this means that pupils have the right to expect a reasonable level of personal privacy.
- The right under Article 8 is not absolute, it can be interfered with but any interference with this right by a school (or any public body) must be justified and proportionate.
- The powers to search in the Education Act 1996 are compatible with Article 8. A school exercising those powers lawfully should have no difficulty in demonstrating that it has also acted in accordance with Article 8. This advice will assist schools in deciding how to exercise the searching powers in a lawful way.