Grange Primary School

E-Safety Policy

Approved: June 2017

Signed:

Review Scheduled: June 2018

Responsibilities

The e-safety co-ordinators are responsible for leading the e-safety program, recording and reporting incidents and liaising with the Local Authority and external agencies to promote e-safety with Grange Primary School.

The member of SLT for e-safety is

- Bev Williams
- Assistant Head

The Governor responsible for e-safety:

- Kelly Booth

The e-safety co-ordinator is:

- Bev Williams
- Steph Oakley
- Supported by Petra Bennett

The school will monitor the impact of e-safety using:

- logs of reported incidents
- Monitoring logs of internet activity
- Internal monitoring data for network activity
- Monitoring walks of the school

Head of School and Senior Leadership Team (SLT)

The Head of School has a duty of care for ensuring the e-safety for members of the school, though the day to day responsibilities will be delegated to the e-safety co-ordinator.

The Head of School and SLT should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against another member of staff **(See flow chart Appendix 1).**

E-Safety Co-ordinator

Takes day to day responsibilities for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy.

Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.

Provides advice for members of staff.

Liaises with the Shrewsbury Academies Trust and the Local Authority.

Liaises with School and Shrewsbury Academies technical staff.

Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Meets with e-safety Governor to discuss and review incidents logs and developing practice.

IT Technician

Is responsible for ensuring the school's technical infrastructure is secure and is not open to misuse or malicious attack.

That the school meets required e-safety technical requirements and implements any new guidance.

That user's only access the networks and devices through a properly enforced password protection.

Teaching and Support Staff

Are responsible for ensuring that they have an up to date awareness of e-safety matters and of the current school e-safety policy and practice.

They have understood, read and signed the staff acceptable use policy.

They report any suspected misuse or problems to the Head of School or e-safety co-ordinator.

All digital communications with pupils, parents and carers should be on a professional level and only carried out using official school systems.

E-safety issues are embedded in all aspects of the curriculum and other activities.

Pupil's understand and follow the e-safety acceptable use policy.

Designated Safeguarding leads (DSL)

Will be trained in e-safety issues and be aware of the potential for serious child protection issues that could arise from:

- Sharing of personal data.
- Access to illegal or inappropriate material.
- Inappropriate online contact with adults and strangers.
- Potential or actual incidents of grooming.
- Cyber-bullying.
- Extremism and radicalisation.

Pupils

Are responsible for:

- Using the schools in line with the school's acceptable use policy.
- Understanding the importance of reporting abuse, misuse and the accessing of inappropriate material

Parents:

Parents and carers play a crucial role in ensuring that children understand the need to use the internet and mobile devices in an appropriate way. The Grange Primary will take every opportunity to help parents understand these issues through newsletters and e-safety campaigns. Parents and carers will be encouraged to support the school in promoting good e-safety practice and follow guidelines on the appropriate use of:

- Digital and video images taken at School events.
- Access to parents' sections of the School website.

Education

For Pupils:

To equip pupils as confident and safe users of the Information Communication Technology (ICT) the school will undertake to provide:

- A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
- Regularly auditing, review and revision of the computing curriculum.
- E-safety resources that are varied and appropriate and use modern technologies to deliver e-safety messages in an engaging and relevant manner.
- Opportunities for pupils to be involved in e-safety education.
- Pupils are taught in all lesson to be aware that the materials and content they access on line needs validating to ensure its accuracy.
- Pupils can develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulation.
- The school actively provides systematic opportunities pupils to develop the skills of safe and using indiscriminative online behaviour.

For Staff:

- All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection and safeguarding procedures.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school's e-safety policy and acceptable use policy.
- All staff have a responsibility to monitor children's safety and well-being whilst using the internet.
- All staff will receive e-safety updates from DSL.
- Teachers will incorporate e-safety values and good working practices to educate pupils to be safe on line.

Internet Use and Acceptable Use Policies (AUP's)

All members of the school community will sign an Acceptable use policy that is appropriate to their age and role. **See appendix 2.**

A copy of the pupil acceptable use policy will be sent to parents with a covering letter and reply slip. **See appendix 3.**

The acceptable use policy will be reviewed annually. All acceptable use policies will be stored centrally in case of breaches of the e-safety policy. The children's acceptable use policy will be stored in the class behaviour file and staff acceptable use policy will be kept in their personal files.

The acceptable use policy will form part of the first lesson of Computing for each year group.

(See appendix 7)

The Prevent Duty:

The Prevent duty is the Duty in the Counter-Terrorism and Security Act 2015 for schools in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The risks affecting children and young people may vary from area to area, and according to their age. Schools are in a prominent position to identify risks within given local context.

Schools should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have a key role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will be integrated into school's ICT curriculum and can be further imbedded in PSHE.

Staff need to be aware of the risks posed by the online activity of extremists and terrorist groups.

The Prevent duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that include:

- Internet searches for terms related to extremism.
- Visits to extremist websites.
- Use of social media to read or post extremist material.
- Grooming of individuals.

This section should be read in conjunction with:

- Grange Primary Prevent Policy.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents and carers is gained if videos or photos of pupils are going to be used on line or outside of school.

If photos or videos are to be used on line, then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents or carers when considering use of images. **See appendix 4**

Staff must always use a school camera to capture images and videos and must not use their own personal devices.

Photos taken by school are subject to the Data Protection Act 1998.

Photos and videos taken by parents or carers

Parents and carers are permitted to take photos and videos of their own children in school events. They are requested not to share photos or videos from school events of social networking sites if other pupils appear in the background.

The parental letter concerning acceptable use policy includes a paragraph concerning posting photos on social networking sites. **See appendix 2**.

Photos for personal use such as those taken by parents or carers are not subject to the Data Protection Act 1998.

Mobile phone and other devices

All staff mobile phones should be switched to silent whilst on the school premises. Pupil phones are to be taken to the school office at the beginning of the school day and collected at the end of the school day. Pupil's found with a phone during the school day will have it confiscated. In this situation the phone must be sent straight to the school office in a sealed envelope that has the pupil's name and class written on. Confiscated phones can be collected by parents or carers at 3:15pm. If this is not possible the child can be given the phone at 3:15pm but their parents will be informed about the incident.

There may be times when some of the features of mobile devices may be beneficial to the learning activities in a lesson (e.g. pupils may wish to capture photos or videos of an experiment). In such cases mobile devices can be used once permission has been granted by the teacher.

If a member of staff suspects that a mobile phone has been misused within the school, then it should be confiscated but the staff should not 'search' the phone. The incident should be passed directly to the SLT who will deal with the matter in line with normal school procedures.

Use of E-mails

Pupils and staff should only use e-mail addresses that have been issues by the school and the e-mail system should only be used for school related matters. Pupils and staff are advised to maintain an alternative personal email address for use at home in non-school related matters. (**See appendix 6-email consent form for pupils**)

Security and passwords

Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always lock the PC if they are going to leave it unattended (press Ctrl-Alt-Delete and select lock screen).

All users should be aware that the ICT system is filtered and monitored.

Data storage

Staff need to risk assess any data they plan to temporarily store on a laptop or USB pen to ensure that any potential loss has minimal impact while we ensure that encrypted laptops and USB are used when necessary.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported. (**Appendix 8**)

Incidents which may lead to child protection issues need to be passed on to a Designated Safeguarding Lead (Charlie Summers, Jo Goddard, Bev Williams) immediately – it is their responsibility to decide on appropriate action not the class teacher.

Incidents that are of concern under the prevent duty should be referred to the designated leads immediately who should decide on the necessary actions regarding safeguarding and the channel panel.

Incidents which are not child protection issues but may require SLT intervention (e.g. cyber bullying) should be reported to the SLT in the same day.

Allegations involving staff must be reported to the Head of School. If the allegation is one of abuse, then it should be handled according to the DFE document titled @dealing with allegations of abuse against teachers and other staff. If necessary, the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. CEOP button, trusted adult, ChildLine)

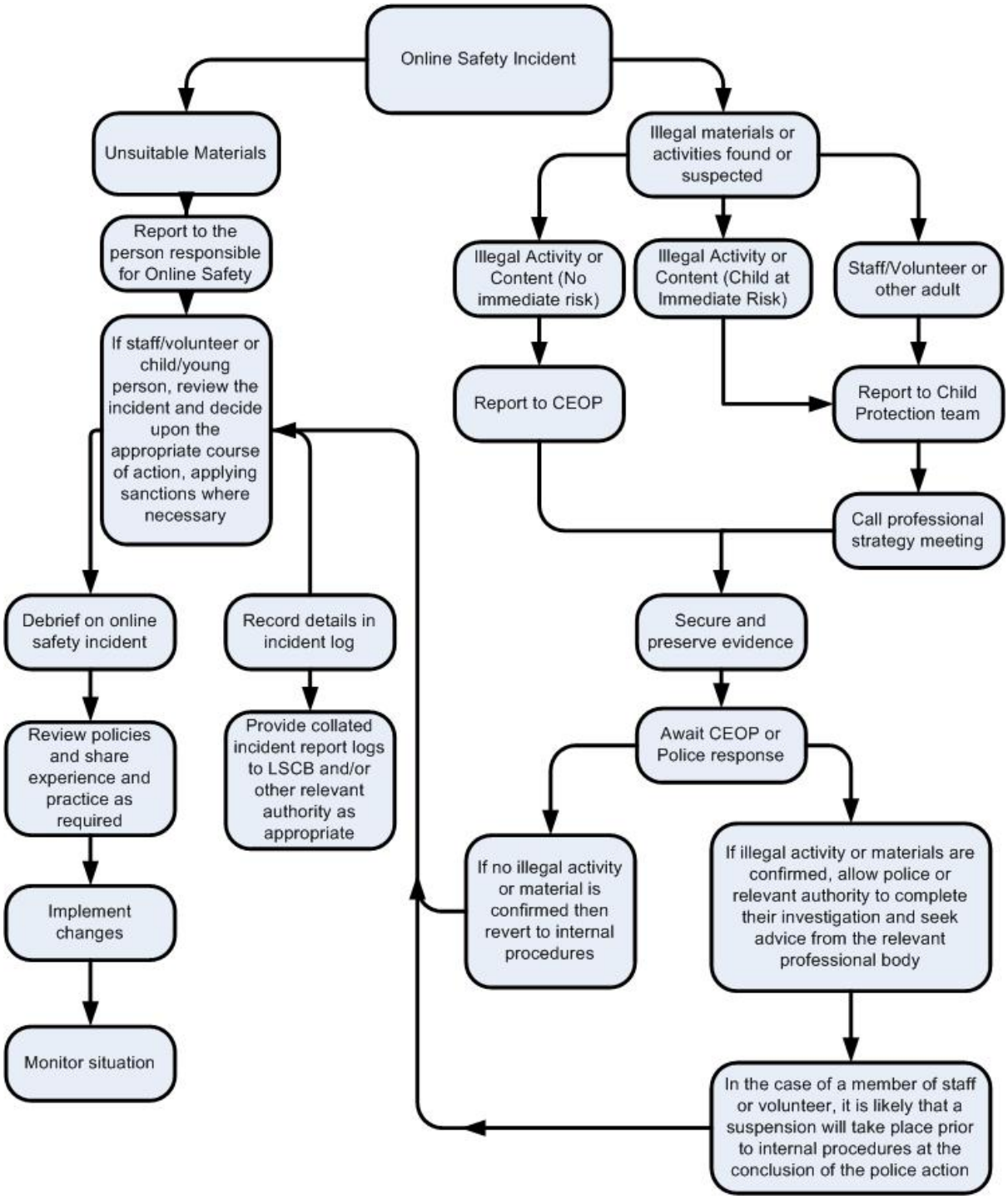
Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages safe and secure approach to the management of the internet. Incidents might involve illegal or inappropriate activities (**see appendix 5 – user actions**)

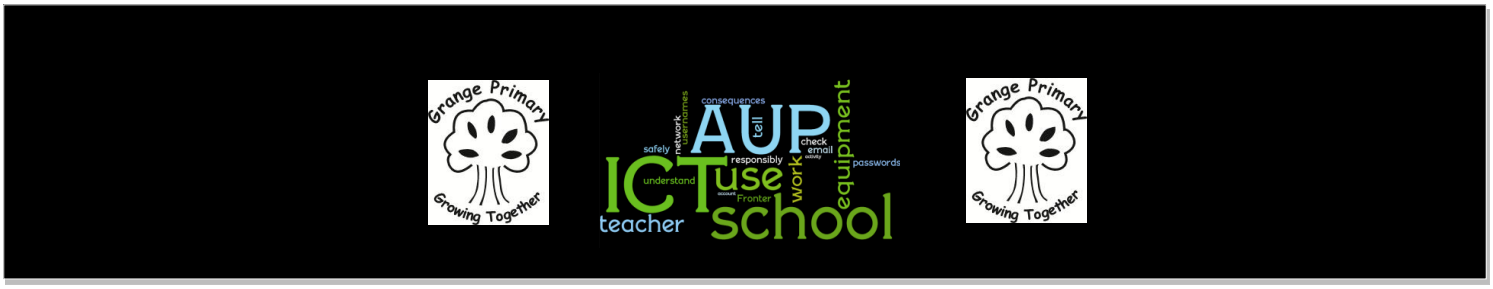
Illegal Incidents

If there is any suspicion that the websites concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart (**appendix 1**) for responding to online safety incidents and report immediately to the police.

Appendix 1 – Flow Chart



Appendix 2



Acceptable Use Policy for Older Primary Children

I will read and follow the rules in the AUP
I understand that this AUP is regularly reviewed and that there are consequences if I do not follow it

- I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy
    - I will never meet an online friend without taking a responsible adult that I know with me.
    - I will always check with a responsible adult before I share images of myself or others.
    - I will always keep my personal details private eg, my real name, mobile phone number, family information journey to school etc.
    - I will discuss and agree my use of a social networking site with a responsible adult before joining
    - 

I am aware of the CEOP report button and know when to use it.
- I will only use school ICT equipment for my school work and not to upset or bully other people or create a bad impression of my school
- I will take responsibility for my own use of all ICT equipment and will use it safely, responsibly and legally eg
    - I will only use my school email account (which ends lg.net) in school
    - I will not open any email attachments without checking with an adult
    - I will make sure that my work does not break copyright
- I will not go on any unsuitable or illegal web sites on purpose e.g. rude images, violence and racism. If I go on any by mistake I will tell a teacher straight away
- I will tell a teacher if I can see a website that is inappropriate or receive any unwanted emails (such as spam)
- I will look after school ICT equipment and report any damage to a teacher straight away
- I will not try to get past any security measures in place to protect the school network
- I will only use the usernames and passwords I have been given and I will keep them secret
- If I have to use a flash drive (USB memory stick) in school I will run an anti-virus check on it before I open my files
- I will save only school work on the school network and will check with my teacher before printing

I understand that all of my work and internet activity on school ICT equipment can be monitored and that there are consequences if I do not use the equipment sensibly, safely and responsibly
I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Parent/Carer's Signature **Date**
Child's Signature

Appendix 3 AUP

Acceptable Use Policy Younger Primary Children

	• I will use school computers for school work and not to upset or be rude to other people. • I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly. • I will log off or shut down a computer when I have finished using it.
	• I will save only school work on the school computer and will check with my teacher before printing.
	• I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy. • I will not tell people about myself online (I will not tell them my name, where I live or anything about my home and family.) • I will not upload photographs of myself without asking a teacher or a trusted adult. • I will never agree to meet a stranger.
	• I will only use my school email account (which ends lg.net) in school. • I will not open emails from people I don't know without checking with my teacher. • I will not open any email attachments without checking with my teacher. • I will show my teacher if I get a nasty message.
	• I will only go on websites that my teacher tells me to. • I will tell my teacher straight away if I go on a website by mistake. • CEOP REPORT ceop.police.uk I am aware of the CEOP report button and know when to use it.

I will read and follow these rules.
I understand that all of my work on school ICT equipment can be seen.
I understand that I must follow these rules or I will be in trouble

Parent/Carer's Signature **Date**

Child's Signature

Appendix 4 – Photo/video consent

GRANGE PRIMARY SCHOOL

CONSENT FORM

Would you please read, complete both sides of this page and sign this form giving your consent for your child to participate in activities during normal school hours at venues other than Grange Primary School during their Educational Years.

I consent to my son/daughter _____(name of child) taking part, if required, in the following activities:-

1. Swimming lessons at Shrewsbury Pool (this is an activity for children in years 3 and 5)

2. Inter school sports activities (venues to be arranged)

3. Play, concerts and shared classroom activities at other schools if appropriate.

4. Places of interest in the vicinity of the school - e.g. local farm, post office, church etc.

   Either walking or transport will be by coach or private car.

If the activity involves less than the whole class, the children may be supervised by a responsible adult, other than a teacher. For all activities pupils will be insured.

We will inform you by letter when any of the above events will be taking place.

Medical Information

* My child does not suffer from any condition requiring regular treatment.

* My child suffers from _____ requiring regular treatment e.g. asthma

I consent to any emergency medical treatment which may be prescribed by a qualified doctor during the course of the visit.

I also consent to any first aid treatment which may be necessary.

Please notify us of any changes in your circumstances that we need to know, e.g. change of address, employment, contact numbers, doctor etc... Please write below. Thank you.

Please read, complete and sign overleaf before returning this form to the school office

School Photographs

Child's Name ……..

We regularly take photographs of children in school participating in a variety of activities. These photographs are usually used in school for displays, in pupils' books and photograph albums.

I agree to school photographs being taken of my child □

I do not agree to school photographs being taken of my child □

Occasionally newspaper photographers call and take photographs of pupils for printing in local papers such as the Shropshire Star and Shrewsbury Chronicle. **These are also likely to appear on the newspaper's online website. Local radio stations occasionally take photos for their website if they are visiting the school.**

I agree to press photographs being taken of my child □

I do not agree to press photographs being taken of my child □

We have a school website – we like to post photographs or video clips of children working, playing or showing their work.

I agree to photographs of my child appearing in the school website □

I agree to video clips of my child appearing on the school website □

I do not agree to photographs of my child appearing on the school website □

I do not agree to video clips appearing on the school website □

Occasionally groups of pupils on trips and visits or participating in workshops have their photographs taken by the leaders and professionals running the activities for the use of brochures, websites or leaflets.

I agree to photographs of my child being taken on visits and during workshops □

I do not agree to photographs of my child being taken on visits and during workshops □

Please be reassured that Staff follow the school safety policy regarding the taking of photographs

Signed (Parent/guardian) _____ Date_____

Appendix 5 – User actions

Pupils

	Incidents: **Class Teacher** should be informed of all incidents. **Red** indicates the actions that must happen in each incidents **X** indicate actions that might happen however any of the actions may be applied if it is considered appropriate.	Refer to class teacher / tutor	Refer to Phase Leader	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
P1	Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X		X		X	
P2	Unauthorised use of non-educational sites during lessons	X	X	X						
P3	Unauthorised use of mobile phone / digital camera / other mobile device	X	X	X			X			
P4	Unauthorised use of social media / messaging apps / personal email	X	X	X			X			
P5	Unauthorised downloading or uploading of files	X	X	X						
P6	Allowing others to access school / academy network by sharing username and passwords		X	X						
P7	Attempting to access or accessing the school / academy network, using another student's / pupil's account		X	X		X	X			
P8	Attempting to access or accessing the school / academy network, using the account of a member of staff		X	X		X	X			
P9	Corrupting or destroying the data of other users	X	X	X		X	X			
P10	Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X			
P11	Continued infringements of the above, following previous warnings or sanctions			X	X		X	X		X
P12	Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X	X		X			X
P13	Using proxy sites or other means to subvert the school's / academy's filtering system			X	X	X				
P14	Accidentally accessing offensive or pornographic material and failing to report the incident			X		X	X	X	X	X

P15	Deliberately accessing or trying to access offensive or pornographic material			X	X	X	X	X	X	X
P16	Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X			X

(b)Staff

Staff **Actions / Sanctions**

	Incidents: **Red** indicates the actions that must happen in each incidents **X** indicate actions that might happen however any of the actions may be applied if it is considered appropriate.	Refer to line managerr	Refer to Headteacher |	Refer to Principal \ HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
S1	Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X		X		X
S2	Inappropriate personal use of the internet / social media / personal email		X				X		
S3	Unauthorised downloading or uploading of files		X	X					
S4	Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account		X			X			
S5	Careless use of personal data eg holding or transferring data in an insecure manner		X						
S6	Deliberate actions to breach data protection or network security rules		X	X		X	X		X
S7	Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X	X		X
S8	Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X		X		X		X
S9	Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X				X		X
S10	Actions which could compromise the staff member's professional standing		X						
S11	Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school / academy		X	X			X		X
S12	Using proxy sites or other means to subvert the school's								

	/ academy's filtering system		X	X		X			
S13	Accidentally accessing offensive or pornographic material and failing to report the incident		X			X			
S14	Deliberately accessing or trying to access offensive or pornographic material		X	X	X	X	X		X
S15	Breaching copyright or licensing regulations		X						
P16	Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X	X

Level 1 infringements (Misconduct) –

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

[Sanction - Head of School. Warning given.]

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

[Sanction – Referred to Head of School / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police.

Other safeguarding actions:

1. Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
2. Instigate an audit of all ICT equipment by an outside agency, such as the school's ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – as detailed on our behaviour policy.

Social networking

Pupils

Pupils are not permitted to use public social networking sites within school

Staff

It is recognised that social networking sites have a major role to play in today's society. However, staff must be aware of the following:

Staff must not add pupils as friends in social networking sites.

Staff must not post pictures of school events without the Head of School's consent

Staff must not use social networking sites within lesson times

Staff need to use social networking in a way that does not conflict with the Department for Education Teacher Standards and the school's Staff Code of Conduct.

Staff should review and adjust their privacy settings to give them the appropriate level of privacy

Staff communication

Staff should only communicate with pupils and parents through official channels. These channels include:

- Post on school letter headed paper
- School telephone system
- School provided mobile phone
- School e-mail system
- School provided video conferencing solutions

The following are excluded from the official channels:

- Social networking sites
- Gaming sites
- Chat rooms
- Personal mobile phones
- Personal e-mail addresses
- Personal video conferencing solutions (eg Skype)

Monitoring and reporting

a). The school network provides a level of filtering and monitoring that supports safeguarding.

b). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

c). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

d). The school action plan indicates any planned action based on the above.

Appendix 6 – Parent letter – internet/e-mail use

THE GRANGE PRIMARY SCHOOL

Bainbridge Green

York Road

Shropshire

SY1 3QR

Telephone 01743 462984
Fax 01743 440343

Head of School - Mrs C Summers

Parent / guardian name:………..

Pupil name: …….

Pupil's registration class:
……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school

I have shared the attached Acceptable Use Policy with my child who has signed it to confirm that they will keep to the school's rules for responsible ICT use. We have returned the signed copy to school and have kept a copy at home.

I understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps

include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community.

I have also read and agree to the policy named '**Social Networking Policy for Governors, Parents, Friends and Volunteers'**

Parent's signature:

Date:

Appendix 7

Grange Primary School
Social Networking Policy for Staff

Introduction
Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook, Myspace or Bebo and posting material, images or comments on site such as You Tube, can have a negative effect on an organisation's reputation or image. In addition, Grange Primary School has a firm commitment to safeguarding children in all aspects of its work. **This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.**

Key Principles
Everyone* at Grange Primary School has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

It is important to protect everyone* at Grange Primary School from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is a key responsibility of all members of staff and it is essential that everyone* considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer **must not communicate** with current pupils from Grange Primary School via social networking.

This policy relates to social networking outside work. Blogging and accessing public social networking sites at work using school equipment is not permitted.

Aims
To set out the key principles and code of conduct expected of all members of staff, governors, friends and volunteers at Grange Primary School with respect to social networking.

To further safeguard and protect children and staff.

Code of Conduct for Everyone* at Grange Primary School – Social Networking (please also refer to the schools e-safety policy).

The following are **NOT CONSIDERED ACCEPTABLE**

- The use of the school's name, logo or any other published material without prior written permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.

- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities without prior written permission from the Headteacher.

In addition to the above, everyone* must ensure that they:

- Do not make any derogatory, defamatory, rude or threatening or inappropriate comments about the school, or anyone at, or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the school's reputation is compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about them which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct
In instances where there has been a breach of the above Code of Conduct, the following will apply: ***Any breaches of this policy will be fully investigated.*** Where it is found that there has been a breach of the policy this may result in action being taken under ***the Disciplinary Procedure.*** A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school

Adopted by Governors: June 2017
Reviewed June 2019

---

* Relating to all members of Grange Primary School – staff, pupils, parents, Governors and all other agencies associated with and work with the school.

Name:……

Signed:…….

Date:…….

Grange Primary School

Social Networking Policy for Staff, Governors, Parents, Friends and Volunteers

Introduction
Social networking activities conducted online outside work, such as blogging (writing personal journals to publicly accessible internet pages), involvement in social networking sites such as Facebook, Myspace or Bebo and posting material, images or comments on site such as You Tube, can have a negative effect on an organisation's reputation or image. In addition, Grange Primary School has a firm commitment to safeguarding children in all aspects of its work. **This policy has been written to set out the key principles and code of conduct that we expect of all members of staff with respect to their responsibilities in connection with the use of social networking sites.**

Key Principles
Everyone* at Grange Primary School has a responsibility to ensure that they protect the reputation of the school, and to treat colleagues and members of the school with professionalism and respect.

It is important to protect everyone* at Grange Primary School from allegations and misinterpretations which can arise from the use of social networking sites.

Safeguarding children is a key responsibility of all members of staff and it is essential that everyone* considers this and acts responsibly if they are using social networking sites out of school. Anyone working in the school either as a paid employee or volunteer **must not communicate** with current pupils from Grange Primary School via social networking.

This policy relates to social networking outside work. Blogging and accessing public social networking sites at work using school equipment is not permitted.

Aims
To set out the key principles and code of conduct expected of all members of staff, governors, friends and volunteers at Grange Primary School with respect to social networking.

To further safeguard and protect children and staff.

Code of Conduct for Everyone* at Grange Primary School – Social Networking (please also refer to the schools e-safety policy).

The following are **NOT CONSIDERED ACCEPTABLE**

- The use of the school's name, logo or any other published material without prior written permission from the Headteacher. This applies to any published material including the internet or written documentation.
- The posting of any communication or images which links the school to any form of illegal conduct or which may damage the reputation of the school. This includes defamatory comments.
- The disclosure of confidential or business-sensitive information; or the disclosure of information or images that could compromise the security of the school.
- The posting of images of employees, children, governors or anyone directly connected with the school whilst engaged in school activities without prior written permission from the Headteacher.

In addition to the above, everyone* must ensure that they:

- Do not make any derogatory, defamatory, rude or threatening or inappropriate comments about the school, or anyone at, or connected with the school.
- Use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the school's reputation is compromised by inappropriate postings.
- Are aware of the potential of on-line identity fraud and to be cautious when giving out personal information about them which may compromise their personal safety and security.

Potential and Actual Breaches of the Code of Conduct
In instances where there has been a breach of the above Code of Conduct, the following will apply: ***Any breaches of this policy will be fully investigated.*** Where it is found that there has been a breach of the policy this may result in action being taken under ***the Disciplinary Procedure.*** A breach of this policy will be considered to be a serious disciplinary offence which is also contrary to the school's ethos and principles.

The Governing Body will take appropriate action in order to protect the school's reputation and that of its staff, parents, governors, children and anyone else directly linked to the school

Adopted by Governors June 2017
Reviewed June 2019

---

* Relating to all members of Grange Primary School – staff, pupils, parents, church, Governors, PTA members and all other agencies associated with and work with the school.

Appendix 8

E safety Incident Record - Pupil

Name of Pupil/pupils involved

_____

Date _____ Time

_____

Incident Number	Incident Details	Action Taken	By whom

This record will be filed in the e safety incident log in the Head of School's office. Copies will be placed in the folder for all involved.

E safety Incident Record - Pupil

Name of Pupil/pupils involved

_____

Date _____ Time

_____

Incident Number	Incident Details	Action Taken	By whom

This record will be filed in the e safety incident log in the Head of School's office. Copies will be placed in the folder for all involved.

E safety Incident Record - Staff

Name of Staff Member involved _____

Date _____ Time _____

Incident Number	Incident Details	Action Taken	By whom

This record will be filed in the e safety incident log and in the teachers file in the Head of School's office. .

E safety Incident Record - Staff

Name of Staff Member involved _____

Date _____ Time _____

Incident Number	Incident Details	Action Taken	By whom

This record will be filed in the e safety incident log and in the teachers file in the Head of School's office. .