



E-Safety Policy

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the <i>Governing Body</i> on:	
The implementation of this e-safety policy will be monitored by the:	<i>SLT</i>
Monitoring will take place at regular intervals:	<i>Annually</i>
The <i>Governing Body</i> will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	<i>Annually</i>
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *Surveys / questionnaires of*
 - *students / pupils*
 - *parents / carers*
 - *staff*

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off Germander Park 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.

Germander Park 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.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within Germander Park:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the *Standards and Progress Committee of the governing body* receiving regular information about e-safety incidents and monitoring reports. A member of the *Governing Body* has taken on the role of *E-Safety Governor*. The role of the *E-Safety Governor* will include:

- *regular meetings with the E-Safety Co-ordinator*
- *regular monitoring of e-safety incident logs*
- *reporting to relevant Governors / Board / committee / meeting*

Headteacher and Senior Leaders:

- **The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community**
- **The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.**
- *The Headteacher and Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.*
- *The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.*

E-Safety Coordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with *E-Safety Governor* to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meeting / committee of *Governors*
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The IT Leader is responsible for ensuring:

- **that Germander Park's technical infrastructure is secure and is not open to misuse or malicious attack**

- **that Germander Park meets required e-safety technical requirements and any LA E-Safety Policy / Guidance that may apply.**
- **that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed**
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher / E-Safety Coordinator

Teaching and Support Staff

are responsible for ensuring that:

- **they have an up to date awareness of e-safety matters and of the current Germander Park e-safety policy and practices**
- **they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)**
- **they report any suspected misuse or problem to the Headteacher for investigation / action / sanction**
- **all digital communications with students / pupils / parents / carers should be on a professional level** and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

Are taught throughout their school life to follow the statements below;

- I only go online with a grown up
- I only click on links and buttons when I know what they do
- I keep my personal information and passwords safe online
- I am kind online
- I always tell an adult/teacher if something online makes me feel unhappy or worried

- I know the school can see what I am doing online
- I have read and talked about these rules with my parents/carers
- I can visit www.thinkuknow.co.uk to learn more about keeping safe online

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Germander Park will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature*. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website / blog

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

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

- **A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and should be regularly revisited**
- **Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities**
- **Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.**
- **Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet**
- **Pupils are taught to report images or materials that make them feel uncomfortable to an adult**
- *Pupils are helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school*
- *Staff should act as good role models in their use of digital technologies, the internet and mobile devices*
- *in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.*
- *Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.*

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website,
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications

Education & Training – Staff / Volunteers

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- **A programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.** It is expected that some staff will identify e-safety as a training need within the performance management process.
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.**
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at external training events (eg from LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation
- Participation in school training / information sessions for staff

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- **Germander Park’s technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of Germander Park’s technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **All users will have clearly defined access rights to Germander Park’s technical systems and devices.**
- **The head teacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations**
- **Internet access is filtered for all users.**
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject’s rights
- Secure
- Only transferred to others with adequate protection.

Germander Park must ensure that:

- **It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.**
- **Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.**
- **All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.**
- **It has a Data Protection Policy**
- **It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)**
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected device

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

- **The official Germander Park email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.** *Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).*
- **Users must immediately report, to the nominated person – in accordance with the school / academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication**
- **Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content.** *These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.*
- Pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Germander Park or local authority liable to the injured party.

Reasonable steps to prevent predictable harm must be in place.

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
-

School staff should ensure that:

- No reference should be made in social media to 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 Germander Park or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X		
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy				X		
Infringing copyright				X		
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X		
Creating or propagating computer viruses or other harmful files				X		
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X		
On-line gaming (educational)				X		
On-line gaming (non educational)				X		
On-line gambling				X		

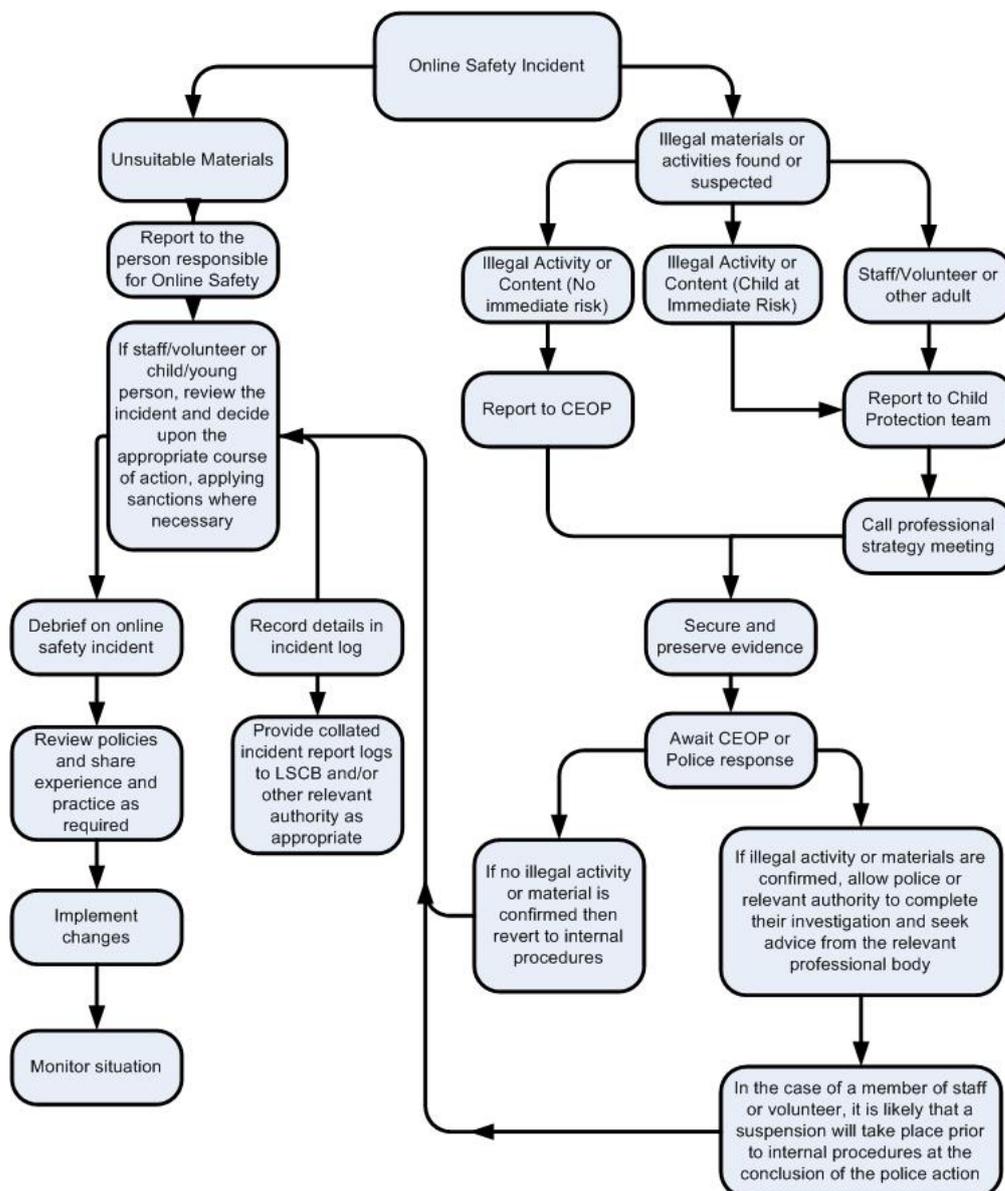
On-line shopping / commerce			X		
File sharing			X		
Use of social media			X		
Use of messaging apps				X	
Use of video broadcasting eg Youtube		X			

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 a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Germander Park policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- **If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:**
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- **Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.**

It is important that all of the above steps are taken as they will provide an evidence trail for the Germander Park and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

It is more likely that Germander Park will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Staff

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
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
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
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	X		
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X			X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X			X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X			X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		X	X					X
Actions which could compromise the staff member's professional standing		X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					X	
Using proxy sites or other means to subvert the school's filtering system	X					X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X					
Deliberately accessing or trying to access offensive or pornographic material				X			X	
Breaching copyright or licensing regulations		X						X
Continued infringements of the above, following previous warnings or sanctions		X					X	X

Pupil Acceptable Use Policy – Germander Park School Parental Acknowledgment

I, with my child, have read and discussed Germander Park School Pupil Acceptable Use Policy.

I am aware that any internet and computer use using school equipment may be monitored for safety and security reason to safeguard both my child and the schools systems. This monitoring will take place in accordance with data protection and human rights legislation.

I with my child, am aware of the importance of safe online behaviour and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community.

I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task. I understand that the school will take all reasonable precautions to reduce and remove risks but cannot ultimately be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities.

I understand that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy or have any concerns about my child’s safety.

I will inform the school or other relevant organisations if I have concerns over my child’s or other members of the school communities’ safety online.

I know that my child will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I will support the schools e-Safety approaches and will encourage my child to adopt safe use of the internet and digital technologies at home.

Child’s Name..... Signed (if appropriate).....

Class..... Date.....

Parents Name.....Parents Signature.....

Date.....

Letter for Staff 2015

Please note this letter does NOT replace a Staff AUP

Dear

Social media can blur the definitions of personal and working lives, so it is important that all members of staff take precautions in order to protect themselves both professionally and personally online.

Be very conscious of both your professional reputation and that of the school when you are online. All members of staff are strongly advised, in their own interests, to take steps to ensure that their personal information and content is not accessible to anybody who does not or should not have permission to access it. All staff must also be mindful that any content shared online cannot be guaranteed to be “private” and could potentially be seen by unintended audiences which may have consequences including civil, legal and disciplinary action being taken. Ensure that your privacy settings are set appropriately (many sites have a variety of options to choose from which change regularly and may be different on different devices) as it could lead to your content accidentally being shared with others.

Be very careful when publishing any information, personal contact details, video or images etc online; ask yourself if you would feel comfortable about a current or prospective employer, colleague, child in your care or parent/carer, viewing or sharing your content. If the answer is no, then consider if it should be posted online at all. It is very important to be aware that sometimes content shared online, even in jest, can be misread, misinterpreted or taken out of context, which can lead to complaints or allegations being made. Don't be afraid to be yourself online but do so respectfully. All staff must be aware that as professionals, we must be cautious to ensure that the content we post online does not bring the school or our professional role into disrepute.

If you have a social networking account, it is advised that you do not to accept pupils (past or present) or their parents/carers as “friends” on a personal account. You may be giving them access to your personal information and allowing them to contact you inappropriately through unregulated channels. They may also be giving you access to their personal information and activities which could cause safeguarding concerns. Please use your work provided email address or phone number to contact children and/or parents – this is essential in order to protect yourself as well as the wider community. If you have a pre-existing relationship with a child or parent/carer that may compromise this or have any queries or concerns about this then please speak to the e-Safety Coordination/Designated Child Protection Lead/Manager.

Documents called “Cyberbullying: Supporting School Staff”, “[Cyberbullying: advice for headteachers and school staff](#)” and “Safer practise with Technology” are available online www.childnet.com, www.kelsi.org.uk and www.gov.uk/government/publications/preventing-and-tackling-bullying. Staff can also visit or contact the Professional Online Safety Helpline www.saferinternet.org.uk/about/helpline for more advice and information on online professional safety.

I would like to remind all staff of our Acceptable Use Policy and the importance of maintaining professional boundaries online. Failure to follow this guidance and the school policy could lead to disciplinary action, so it is crucial that all staff understand how to protect themselves online. Please speak to your line manager, the school e-Safety/child protection lead or myself if you have any queries or concerns regarding this.

Yours sincerely,

Headteacher

Additional content regarding online participation on behalf the School

The principles and guidelines below set out the standards of behaviour expected of you as an employee of the school. If you are participating in online activity as part of your capacity as an employee of the school then we request that you:

•

- Be professional and remember that you are an ambassador for the school. Disclose your position but always make it clear that you do not necessarily speak on behalf of the school.
- Be responsible and honest at all times and consider how the information you are publishing could be perceived
- Be credible, accurate, fair and thorough.
- Always act within the legal frameworks you would adhere to within school, including libel, defamation, confidentiality, copyright, data protection as well as equalities laws.
- Be accountable and do not disclose information, make commitments or engage in activities on behalf of the school unless you are authorised to do so.
- Always inform your line manger, the school e-Safety lead and/or the head teacher of any concerns such as criticism or inappropriate content posted online.

Germander Park Staff Acceptable Use Policy 2015

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites.
2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.
4. I will respect system security and I will not disclose any password or security information and will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be taken and used as stated in the school image use policy and will always take into account parental consent.
7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the School shared drive to

upload any work documents and files in a password protected environment I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
9. I will respect copyright and intellectual property rights.
10. I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces
11. I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (**Verity Stobart**) and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Child Protection Coordinator and/or the e-Safety Coordinator and/or the designated lead for filtering as soon as possible.
12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team/lead as soon as possible.
13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.
14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.
15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.
16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.
17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Child Protection Coordinator and/or the e-Safety Coordinator (or the Head Teacher).

18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: Print Name: Date:

Accepted by: Print Name: