Online Safety Policy
Grangefield School

Approved by:	Governors	**Date:** 10th January 2022
Last reviewed on:	5th January 2022	
Next review due by:	January 2023	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy links closely to the Safeguarding Policy.

This policy links closely to and is referenced within the Grangefield School Staff and Volunteer Acceptable Use Policy Agreement which staff and regular volunteers (where relevant) sign. (see Appendix 3A)

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Dave Turl

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy. At Grangefield School the head teacher is the DSL and the Deputy Head Teacher is a deputy DSL.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the SMT in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the SMT, Computing Subject leader, IT technician and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged on CPOMs and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 ICT Support technician

The ICT Support Technician is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently in all platforms of communication with staff and parents
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (see Appendix 3A and B) and ensuring that pupils follow the school's terms on acceptable use (appendix 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendix 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3b).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during information evenings to parents'.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

When appropriate and relevant, the school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in this policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1, 2 and 3). Staff and regular volunteers do this within the Grangefield School Staff and Volunteer Acceptable Use Policy Agreement. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

In Years 5 and 6, pupils may bring mobile devices into school for the sole purpose of having a form of contact in walking to and from school, but are not permitted to use them during:

- Lessons
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

9. Staff using devices

9.1 Staff using work devices outside of school

Staff members using a work device outside school should only install educational software from a reliable provider on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the IT Technician.

Work devices must be used solely for work activities.

9.2 Staff using own devices for school purposes

Staff are allowed to use mobile phones to call the emergency services if the need arises.

Staff are allowed to use mobile phones to call parents in a medical capacity, where necessary. This is in agreement with the parent in must be made clear that it is within school hours only.

Staff can access their emails using other devices but need to try and keep a work/life balance. Using the app for email is preferable to accessing through the internet.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. This is carried out via CPOMS (the schools online portal used for Safeguarding and behaviour within the school).

This policy will be reviewed annually by the IT Lead and SMT. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-Bullying Policy
- Staff disciplinary procedures and Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure
- Grangefield School Staff and Volunteer Acceptable User Policy Agreement (see Appendix 3)

14. The use and publishing of photos

Staff will follow these processes when using photos within school and the platforms of communicating with parents.

- Photographs that include pupils will be carefully selected and used in accordance with parental requests
- Pupil's full names will never be used in association with any photograph
- Permission from parents/carers has been obtained before photographs of pupils are used via a Photograph Permission on-line form – this is to be updated on an annual basis

Appendix 1: Acceptable use agreement (KS2 pupils and parents/carers)

Acceptable use of the school's IT systems and internet: agreement for KS2 pupils and parents/carers	
Name of pupil:	
When using the school's IT systems and accessing the internet in school, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Access any inappropriate websites • Access social networking sites • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share my password with others or log in to the school's network using someone else's details • Give my personal information (including my name, address or telephone number) to anyone without the permission of my teacher or parent/carer If I bring a personal mobile phone or other personal electronic device into school: • I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online I agree that the school will monitor the websites I visit. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the school's IT systems and internet responsibly.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: Acceptable use agreement (EYFS & KS1 pupils and parents/carers)

<table>
<tr><th colspan="2">Acceptable use of the school's IT systems and internet: agreement for KS2 pupils and parents/carers</th></tr>
<tr><td colspan="2">Name of pupil:</td></tr>
<tr><td colspan="2">When using the school's IT systems and accessing the internet in school, I will:
Not use the internet without a teacher being present
Click on links and buttons when I know what they do
Always ask if I get lost on the internet
Open emails together with a teacher or trusted adult
Use kind language when I email people
Not share my password with others
I agree that the school can monitor the websites I visit.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's IT systems and internet responsibly.</td></tr>
<tr><td>Signed (pupil):</td><td>Date:</td></tr>
<tr><td colspan="2">Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet.</td></tr>
<tr><td>Signed (parent/carer):</td><td>Date:</td></tr>
</table>

Appendix 3a: Grangefield School Staff and Volunteer Acceptable Use Policy Agreement (staff and regular volunteers)

This policy has been written in collaboration with all staff employed by the school. Its aim is to safeguard staff against risks posed to themselves and to those in their care through digital technology. Because of the speed of emerging technology, the policy will be reviewed and signed annually by all school staff and those training within the school.

Access

- I will keep any school related user names and passwords confidential. (Please note that Head Teacher, Administrator and IT Technician know where log–in details and passwords can be found in case of absence. They will only be used in extenuating circumstances).
- If I believe other persons may have gained access to my log-in and password details, I will inform the IT subject leader and the person with responsibility for e-safety so that they can be changed.

Content

- When on the school premises or using school equipment, I will not browse or download material that could be considered inappropriate or offensive to pupils, colleagues, parents or those from the wider school community.
- I will report any accidental access to illegal, inappropriate or harmful materials to the person responsible for e-safety.
- I will not download any software or resources from the Internet that can compromise the network; or that are not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I understand that Internet usage will be logged and this information could be made available to the Head Teacher on request.
- I accept that any laptop or IPAD loaned to me by the school; remains the property of the school and is provided to support my professional role but may also be used for responsible personal use. (The rules set out in this agreement also apply to use of school IT systems out of school).
- I will not use personal memory cards or camera phones to take or transfer images of pupils or colleagues.
- I agree not to download images of pupils and colleagues onto my personal equipment.
- I will only access and store sensitive/personal data and information on the school network, accessed through central hosting, and not on a local drive or memory stick.
- I will respect copyright and intellectual property rights whenever accessing online material.
- When I use my personal hand held/external devices (mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will only use social networking sites in school when using a personal device and only during break times; when no pupils are present.
- I understand that this policy sits alongside the On-Line Safety Policy which aims to educate about and protects the on-line safety of pupils, staff, volunteers and governors, within the school community.

Contact

- I will not send any communication to others within my professional community that could reasonably be considered offensive. This specifically includes, but is not exclusive to bullying and abuse.
- When communicating by e-mail on school business, I agree to only use the secure, county e-mail address, to ensure the protection of data and personal information.
- I will use the school office e-mail address, Tapestry or Class Dojo to communicate with parents and carers, not my personal or professional e-mail address.

- I agree to contact colleagues on their personal mobile phones only if they have given me prior permission to do so.
- When off-site, (for example on day visits and residential trips) I agree to contact parents/carers etc. using the trip site phone or school mobile phone whenever possible, only using my personal one (with the number blocked) in an emergency.
- I understand that I should not contact parents or pupils using my mobile phone, or give them access to my personal mobile phone number, except in an emergency. (On occasions, there may be mitigating circumstances where parents are also friends and may be contacted through friendship – not professionally. In these circumstances, staff should discuss this with the Head Teacher and the details noted on page 3 of this agreement which will be kept securely in the school office. In the circumstance of it being the Head Teacher who has friends who are also parents, the head should inform the Governor with responsibility for e-safety and the details noted in the same manner.)
- I agree that I will not make contact with pupils, parents or carers through a social networking site (or similar) and will ensure maximum security settings to prevent, as far as possible, pupils, parents and carers gaining access to my profile. (On occasions, there may be mitigating circumstances where parents are also friends and may be contacted through friendship – not professionally. In these circumstances, staff should discuss this with the Head Teacher and the details noted on page 3 of this agreement which will be kept securely in the school office. In the circumstance of it being the Head Teacher who has friends who are also parents, the head should inform the Governor with responsibility for e-safety and the details noted in the same manner.)

Commerce

- I will not advertise or sell my services through digital technology connected in any way with the school.
- I will not access any gambling, auction or commercial sites during school working hours or in view of pupils, except in exceptional circumstances agreed by the Head Teacher. The Head Teacher will agree this with the relevant governor.
- I agree not to subscribe to any services, sites or goods on behalf of school without first asking for the permission of the relevant budget holder.

General

- I will not allow unauthorised individuals to access Email / Internet / Intranet etc.
- I will only use LA systems in accordance with any Corporate policies.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.
- I understand that family members and friends should not be allowed to use school equipment.
- I understand that I will be held responsible for any misuse of a laptop, or other school equipment issued to me.

Safeguarding

- If interacting with pupils on-line while working from home (Remote Learning), I will continue to follow existing school policies, with particular reference to Staff Code of Conduct, IT Acceptable Use Policy, On-line Safety Policy, the Safeguarding Policy and Annexes to the Safeguarding Policy (Covid 19 and Remote Learning), and to follow DFE guidance in Annex C of KCSiE.

I agree to abide by the Grangefield School Acceptable Usage Policy.

Signed _____ Print name _____Date _____

2 copies of this AUP should be signed.

One copy to be retained by the member of staff, the second to be kept in the e-safety file.

Mitigating circumstances: (where the staff member is a parent at Grangefield who knows many parents in their child's class, indicate the year group and class of your child rather than each individual parents.)

Please tick if you have discussed and/or recorded any "mitigating circumstances", as mentioned above, with the Head Teacher/Governor	

Appendix 3b: Grangefield School Acceptable Use Policy Agreement (governors, occasional volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for governors, occasional volunteers and visitors	
Name:	
When using the school's IT systems and accessing the internet in school, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software • Share my password with others or log in to the school's network using someone else's details	
I will only use the school's IT systems and access the internet in school, for educational purposes or for the purpose of fulfilling the duties of my role. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (governor/visitor):	**Date:**

Appendix 4: Online safety training needs – Self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's IT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	