Scott

Scott Medical and Healthcare College

Online Safety Procedure

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 procedure is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2025, and its advice for schools on:

https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff

Relationships and sex education

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.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this procedure 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).

All governors will:

Ensure that they have read and understand this procedure

Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

3.2 The Headteacher

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

3.3 The designated safeguarding lead (DSL)

Details of the school's DSL and Safeguarding Team are set out in our child protection and safeguarding policy as well relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this procedure and that it is being implemented consistently throughout the school
- Working with the Headteacher, IT Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 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 The IT Manager

The IT Manager 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 ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure secure user authentication and access controls.
- Manage data backup and disaster recovery processes.
- Ensure compliance with legislation such as GDPR, the Data Protection Act, and safeguarding guidelines.
- 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 procedure
- Implementing this procedure consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged CPOMs and dealt with appropriately in line with this procedure
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Complete regular self audit to update knowledge and assess training needs

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

What are the issues? - UK Safer Internet Centre

Hot topics - Childnet International

Parent factsheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this procedure, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

RSHE covers modules on consent, emotional wellbeing and bullying which are linked to online behaviours.

Curriculum collapse programmes cover healthy relationships, e-safety and risky behaviour.

As part of their Key Stage 3 Computing Curriculum in Year 7 and 8, students learn about online safety. In Year 7, students learn how to keep their personal information secure through the use of strong passwords and careful use of services such as social media. Students learn how to report concerns and use a variety of communication tools, such as email appropriately. This is reinforced throughout their Computing Curriculum in Year 7 and 8 and through their use of technology in other curriculum areas.

In Key Stage 4, students have the opportunity to learn about topic areas such as Computer Security where themes such as viruses, hacking, phishing and social engineering are discussed, as well as ways to prevent these risks, legal, ethical, environmental and cultural issues relating to technology are also discussed. Students learn how to protect their privacy and identity through tools such as strong passwords, encryption, anti-malware software.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology (including AI) safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Recognise inappropriate content, contact and conduct, and know how to report concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*
- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

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

The school will use a variety of methods including 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 procedure will also be shared with parents.

Online safety will also be covered during parents' evenings.

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

Concerns or queries about this procedure 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. (See also the safeguarding and school behaviour policy.)

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. Tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies, curriculum sessions and during curriculum collapse .

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, relationship, sex and health education (RSHE) 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 (see section 11 for more detail).

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 the school behaviour policy and anti bullying procedure. 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 the Plymouth Children’s Social Care 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, the DSL or a 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.

If there is thought to be sexually inappropriate images of children on the device it should not be viewed under any circumstance and be reported to the DSL immediately.

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 . 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.

8. Children and online safety AWAY from school and college

Scott Medical and Healthcare College will do what we reasonably can to keep all of our children safe online.

All staff who interact with children, including online, will continue to look out for signs a child may be at risk. Any such concerns will be dealt with as per the child protection policy and where appropriate referrals will still be made to other agencies, children's social care and, as required, the police.

Scott Medical and Healthcare College will consider the safety of children when they are asked to work online, the starting point for which will be that the same principles as set out in Scott Medical and Healthcare College**Staff code of conduct** and **acceptable user policy.** Additional guidance for staff working 'online' with children have been shared with staff in a document titled: **Managing an online meeting with children (Appendix 2)**. This has been shared with all staff.

The procedures outlined apply equally to any existing or new online and distance learning arrangements which are introduced. Functions of online platforms also restrict students' use of google meet without a teacher present for example.

Scott Medical and Healthcare College will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. Students can report any concerns to *safeguarding@sdcc-smhc.net*

As well as reporting routes back to Scott Medical, our website includes signposting children to age appropriate practical support from the likes of:

Childline - for support
UK Safer Internet Centre - to report and remove harmful online content
CEOP - for advice on making a report about online abuse

Scott Medical and Healthcare College will attempt to maintain regular contact with parents and carers and these communications will be used to reinforce the importance of children being safe online.

Scott Medical and Healthcare College will make parents and carers aware through our Web Page of what their children are being asked to do online, including the sites they will be asked to access and be clear who from Scott Medical and Healthcare College (if anyone) their child is going to be interacting with online.

Parents and carers will be responsible, where a family deems they wish to engage additional support from an outside individual to assist in their child's learning, for securing this support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school, however only 6th form students are permitted to use them:

- Within school buildings at any time after 08:35, unless directed by the teacher for the purpose of enhancing learning.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

- Mobile phones are allowed to be brought to school for safety reasons but must remain in bags and switched off. We have a 'hear it, see it, lose it' procedure and any mobile phones infringement will result in the collection by the Oncall Team, stored in the school safe for Parents to collect.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

10. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

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 Manager.

Work devices must be used solely for work activities.

All Staff agree and sign the Greenshaw Learning Trust Code of Conduct at the start of each academic year or start of service.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and acceptable user policies. 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 ICT 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/staff code of conduct. 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 and the Local Area Designated Officer LADO.

12. 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 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.

13. Monitoring arrangements

The Staff and DSL logs behaviour and safeguarding issues related to online safety on CPOMS. An incident report log of any serious incidents will be provided to the Headteacher team and the Local Governing Body (LGB).

This procedure will be reviewed every year by the DSL working with the IT Manager at every review, the procedure will be shared with the governing board.

14. Links with other policies

This online safety procedure is linked to our:

Child protection and safeguarding policy

Behaviour policy

Staff disciplinary procedures

Staff Code of Conduct

Data protection policy and privacy notices

Complaints procedure

Appendix 1: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and internet: agreement for staff, governors,volunteers and visitors
Name of staff member/governor/volunteer/visitor:
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: · Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) · Use them in any way which could harm the school's reputation · Access social networking sites or chat rooms other than for professional duties. · Use any improper language when communicating online, including in emails or other messaging services · Install any unauthorised software, or connect unauthorised hardware or devices to the school's network Make the DSLor Network Manager aware if I become a victim of or if my data has been compromised by a cyber attack (phishing scam, ransomware attack, etc) · Share my password with others or log in to the school's network using someone else's details · Take photographs of pupils without checking with teachers first · Share confidential information about the school, its pupils or staff, or other members of the community · Access, modify or share data I'm not authorised to access, modify or share · Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that digital communication with students will always be on a professional level and only carried out using official college systems, these are - College email, Google drive, or Google Classroom. Google Meet should not be used to communicate with students but may be allowed for the purpose of teaching during imposed school closure (e.g. due to COVID19). I understand that guidelines for such exceptional use will be issued by the DSL and SMT and I agree to abide by them and record all such sessions for safeguarding purposes. I understand that the use of this facility will be restricted to specific year groups. Phone calls home will also be permitted to check on welfare during imposed school closure; I understand that the phone calls should only be undertaken using the College 3CX system which automatically records the conversation for safeguarding purposes.

I understand that phone calls using the College 3CX system are recorded for safeguarding purposes.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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 procedure and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and IT Manager 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 ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 2:Managing an online meeting with children

Expectations and protocols

1. Be mindful that the principles of **Keeping Children Safe In Education** continue to apply at all times. Familiarise yourself with the revised arrangements outlined in the **new addendum** to the college's **Child Protection & Safeguarding Policy**.

2. Consider and apply the principles outlined in the **Staff Code of Conduct** and the **Acceptable User policy** which underpin the safety of children and staff working online.

3. Apply the **principles of data protection** and ensure that you are safeguarding students' information particularly during online meetings. You should always use school provided email addresses; telephone calls should be made via the 3CX phone system.

4. **Meetings should be conducted within the normal hours of the working day (8.30am - 5.30pm)**

5. **Only the teacher must set up the meeting (do not join a meeting set up by a student)**

6. Consider the location of the meeting, having your camera set up in a bedroom is **not** appropriate; similarly it would not be appropriate for the child to be speaking with you from their bedroom. If there are no alternative locations available, cameras should be turned off.

7. **Ensure that professional standards are maintained at all times ie**
    a. **ensure that you are dressed appropriately,**
    b. **the visual background of your workstation is as neutral as possible**
    c. **a classroom standard of behaviour is expected and practised by all participants.**
    d. **Other members of your household should not be present during these meetings (e.g another adult, not a staff member; your children)**

8. **All meetings should be recorded by the teacher, and kept in the shared drive. You must tell all parties that the meeting is being recorded.**

9. **There should always be a minimum of 2 adults on any online meeting where possible.** If this is not possible the meeting will be recorded to safeguard all

involved. It is not expected that there will be two members of staff in counselling sessions.

10. Be prepared for the meeting; have a list of items you wish to discuss and work through the list. Make clear at the beginning the purpose of the meeting.

11. Establish and follow the etiquette guidelines as for meetings with colleagues.

12. Be clear and concise and ensure the student (and/or parent/carer) understands your questions.

13. Make notes of responses and any actions required as a result of the meeting.

14. If you think the child with whom you are communicating may be at risk or if you become aware of any safeguarding or other concerns, report immediately using the normal channels as detailed in the Child Protection and Safeguarding Policy **and** log your concern on CPOMS. Plymouth Gateway Service can be contacted on 01752 668000; select Option 1 – Children's Services. Alternatively, you can email the Plymouth Gateway Service at: gateway@plymouth.gov.uk. You can also contact the NSPCC helpline on 0808 800 5000. If a child, young person or an adult is at **immediate** risk of harm, please contact **999**.

15. Ensure that the student understands how to report any concerns that might arise when they are working online, ie reporting back to the college and signpost age appropriate practical support from:

    a. Childline for support: https://www.childline.org.uk/?utm_source=google&utm_medium=cpc&utm_campaign=UK_GO_S_B_BND_Grant_Childline_Information&utm_term=role_of_childline&gclsrc=aw.ds&&gclid=EAIaIQobChMIlfLRh-ez6AIVRrDtCh1N9QR2EAAYASAAEgLc-vD_BwE&gclsrc=aw.ds

    b. UK Safer Internet Centre - to report and remove harmful online content

       https://reportharmfulcontent.com/

    c. CEOP - for advice on making a report about online abuse

       https://www.ceop.police.uk/safety-centre/