Online Safety Policy

September 2023

Next Update: September 2024

Approved by: Chair of Trustees

Principal: Neil Bain

Designated Safeguarding Lead

Contents

1. Aims

Wemms Education Centre aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, external partners and Trustees.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

1.1 Definitions

The four key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying etc.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scamming.

These categories are not exclusive and may be revised and added to as categories of risk are further identified.

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education 2022, Keeping Children Safe in Education 2023 and its advice for schools on:

- 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
- Filtering and Monitoring

It also refers to the DfE'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 Principal

The Principal has overall responsibility for monitoring this policy and is accountable for its implementation.

The Trustees have a role to advise the Principal and 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 Principal and staff will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND because of the importance of recognising that a *'one size fits all'* approach may not be appropriate for all children in all situations and a more personalised or contextualised approach may often be more suitable.

3.2 The Senior Management Team (SMT)

The SMT is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school and within their departments.

3.3 The Designated Safeguarding Lead (DSL)

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

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

- Supporting the SMT and ICT manager in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

- Working with the SMT, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged, reported on MYCONCERN and dealt with appropriately in line with this policy.
- 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.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Principal and/or the Trustees.

This list is not intended to be exhaustive, and roles may be extended as required.

3.4 The ICT Contractor

The ICT contractor is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems. These are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept 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 weekly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Implementing the login procedures including the use of personal security code generators.

This list is not intended to be exhaustive.

3.5 All Staff and Volunteers

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

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use.
- Working with the DSLs to ensure that any online safety incidents are logged 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.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of *'it could happen here'*.
- Maintaining the security of their own social media and internet presence such that it does not breach the Teacher's Standards or bring the Teaching profession into disrepute.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal 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 ICT systems and internet.

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 resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 Visitors and Members of the Community

In general, visitors and members of the community are unable to access the school's ICT systems, although in circumstances where visitors and members of the community request use of the school's ICT systems or internet, they 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.

4. Educating Students about Online Safety

Students will be taught about online safety as part of the curriculum, in ICT lessons, Web Design lessons, as part of PSHE and Citizenship classes and as part of other lesson such as Preparation for Post-Wemms and Careers. Assemblies will also be used to remind students about online safety when appropriate.

Acknowledgement is also made of the guidance on relationships education, relationships and sex education (RSE) and health education since **All** schools must teach:

- Relationships education and health education in primary schools.
- Relationships and sex education and health education in secondary schools.

At Wemms Education Centre, we aim to teach the following as appropriate to our student intake:

In **Key Stage 1**, students 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.

Students 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.

By the **end of Middle School**, students will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
- How information and data is shared and used online.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.

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

- Understand a range of ways to use technology 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.
- How to report a range of concerns.

By the **end of Secondary School**, students 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.
- How people can actively communicate and recognise consent from others, including sexual consent and how and when consent can be withdrawn (in all contexts, including online).

At Wemms Education Centre, the safe use of social media and the internet will also be covered in other subjects where relevant such as Drama, PSHE, Citizenship classes, Toastmasters and Assemblies.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents about Online Safety

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

Online safety will also be covered during parents' meeting and all parents will be invited to participate in an online safety briefing/course.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL/DDSL.

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

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 students understand what it is and what to do if they become aware of it happening to them or others.
- We will ensure that students 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 students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying within PSHE/Citizenship and other relevant classes.
- Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes but is not restricted to personal, social, health and economic (PSHE) education, Web design, Office 365, ICT, coding and other subjects where appropriate.
- All staff, Trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, 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. Where illegal, inappropriate or harmful material has been spread among students, 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 students' 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 management 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*

* Staff may also confiscate devices for evidence to hand to the police, if a student's discloses that they are being abused and that this abuse includes an online element.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's risk assessments including those related health and safety and to COVID-19.

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

7. Acceptable use of the Internet in School

- All students, parents, staff, volunteers and Trustees 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 students, staff, volunteers, Trustees and visitors (where relevant) to ensure they comply with the above.

8. Students using Mobile Devices in School

Students may bring mobile devices into school, but are not permitted to use them during:

- School hours 8.30 am to 4.00 pm.
- Using mobiles phones as an education device in lessons is not permitted.
- Break and lunch times. If the student needs to speak to their parents, they may use the school phone having received permission from Head Of Student Services, or another senior member of staff.
- Mobile phones are not permitted in assemblies or any small group time (e.g. year groups)

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

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

9. Staff using Work Devices outside School

All staff members will take appropriate steps to ensure their devices remain secure. This includes but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.

- Keeping operating systems up to date – always install the latest updates.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL and or the ICT contractor.

In general, all updates will be implemented by the ICT contractor who will have admin rights for downloading and installing software. No Teachers or Students will have admin rights unless approved by the Principal for the purposes of completing their duties as a member of staff.

10. How the School will Respond to Issues of Misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. 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 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.

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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.

- Sharing of abusive images and pornography, to those who don't want to receive such content.

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse.
- develop the ability to ensure students can recognise dangers and risks in online activity and can weigh the risks up.
- develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL, Deputy DSL and SMT 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 about online safety at regular intervals, and at least annually.

Trustees 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 using the school's My Concern system.

This policy will be reviewed every year by the DSL and SMT. At every review, the policy will be shared with the Trustees for comment. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

This online safety policy relates to:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Code of Conduct
- Whistleblowing Procedures
- Anti-Bullying Policy
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy
- Exclusions Policy
- Staff Discipline, Conduct and Grievance Policy

- Policy for Dealing with Allegations Against Staff
- Curriculum Policy
- Wemms Ethos Policy
- British Values Policy
- Site Security Procedure
- Health and Safety Policy
- DSE Assessment Policy
- Risk Assessment Policy