DROITWICH SPA HIGH SCHOOL AND SIXTH FORM CENTRE

life. Changing. learning.

ONLINE SAFETY POLICY

Reviewed:	May 2025
Next Review:	May 2026
Person Responsible for policy:	DCC

Contacts

Internal

Senior designated persons for Child Protection and persons who act in the absence of the senior designated person

Mr J. D. Broughton (Senior Leader/Head of student welfare), Mrs G. Lloyd-Davies (Co-Headteacher and Deputy Safeguarding Lead), Mr A. M. Ward (Senior Leader and Deputy Safeguarding lead) and Mr D. C. Corbett (Online safety Coordinator)

Mrs K Moore

Governor responsible for safeguarding children

External

Senior Adviser for Safeguarding Children in Education	01905 728902
Children's Services Access Centre	01905 768054
Out of Hours Emergency Duty Team	01905 768020
Police Public Protection Unit:	
24hrs non-emergency	0300 333 3000
Emergency	999
NSPCC Helpline	0808 800 5000

1. Introduction

1.1 Droitwich Spa High School recognises that internet use is an essential tool for learning. Access to the internet is an entitlement for students who show a responsible and mature approach to its use. Students use the internet widely outside school. They need to learn how to evaluate information and to take care of their own safety and security.

1.2 The Online Safety Policy provides an important part of the school's safeguarding provision for students. This policy also relates to other school policies including those for:

- Behaviour and discipline
- Anti-bullying (including cyberbullying)

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

1.4 The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other online safety incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The Counter-Terrorism and Security Act 2015 places a legal duty on schools to prevent people from being drawn into terrorism through the internet or other means, and to challenge extremist views.

1.5 The school will deal with such incidents in accordance with this policy and associated behaviour and anti-bullying policies and will inform parents/ carers of known incidents of inappropriate online safety behaviour that take place out of school.

2. School Commitment

2.1 The school adopts an open and accepting attitude towards children as part of its responsibility for pastoral care. The Staff endeavour to ensure that children and parents will feel confident in discussing any concerns, reporting any incidents and will see school as a safe place when these concerns or incidents will be dealt with efficiency and effectiveness. Children's worries and fears will be taken seriously and children are encouraged to seek help from members of staff. Children will feel safe and be well equipped to manage risks and feel confident in reporting online safety concerns.

2.2 The school will therefore:

- establish and maintain an ethos where children feel secure and are encouraged to talk, and are listened to;
- ensure that children know that there are adults in the school whom they can approach if they are worried or are in difficulty;
- ensure every effort is made to establish effective working relationships with parents and colleagues from other agencies;
- Operate safe recruitment procedures and make sure that all appropriate checks are carried out on new staff and volunteers who will work with children, including references, DSB checks and ISA registration.

3. Roles and Responsibilities

3.1 General

All adults working with or on behalf of children have a responsibility to safeguard and promote the welfare of children. This includes a responsibility to be alert to possible abuse and to record and report concerns to staff identified with child protection responsibilities within the school.

An effective whole-school approach to online safety will be implemented by the school to protect and educate pupils, students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

An annual review to our approach to online safety will be supported by an annual risk assessment that considers and reflects the risks that children face.

3.2 Roles and responsibilities of the Governing Body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This responsibility will be discharged by the Governors receiving regular information about online safety incidents and monitoring reports. The governor with responsibility for Safeguarding Children will also liaise with the Head of student welfare and the Headteacher in order to provide information and reports to the Governing Body when appropriate. The Governing Body has a responsibility to ensure staff receive regularly updated training which now includes specific mentions of online safety. The Governing Body will ensure the school meets the DfE's Filtering and Monitoring Standards, with clear oversight, regular review, and recording of decisions regarding filtering/monitoring provision.

3.3 Roles and Responsibilities of the Headteacher

The Headteacher of the school will ensure that:

- the policies and procedures adopted by the Governing Body are fully implemented, and followed by all staff;

- the Online safety Coordinator, Head of student welfare and other relevant staff are allowed sufficient time and resources to be suitably trained and are able to train other colleagues, as relevant;
- at least one other member of the Senior Leadership Team is aware of the procedures to be followed in the event of a serious Online safety allegation being made against a member of staff;
- the Senior Leadership Team receives reports from the Online safety Coordinator/Head of student welfare when appropriate.

3.4 Roles and responsibilities of the Head of student welfare

The head of student welfare will:

- assist in embedding online safety in staff training and their continuing professional development
- act as a key point of contact on all online safety issues and have a lead role in establishing and reviewing the school online safety policy documents;
- raise awareness and understanding of online safety to all stakeholders, including parents/ carers;
- liaise with the ICT systems manager and ICT support staff;
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- be responsible for the discipline and guidance of those students involved with an online safety issue, working alongside the pastoral team wherever necessary.
- establish and communicate clear escalation routes for online safety concerns, ensuring all staff and pupils know who to contact and how incidents are handled.

3.5 Roles and responsibilities of the Online Safety Coordinator

The Online Safety coordinator will:

- develop an e-safe culture throughout the establishment
- Embed online safety in staff training, continuing professional development and across the curriculum and learning activities, ensuring all activities and online safety topics are up to date and relevant.
- act as a key point of contact on all online safety issues and have a lead role in establishing and reviewing the school online safety policy documents;
- raise awareness and understanding of online safety to all stakeholders, including parents/ carers;
- liaise with the ICT systems Manager and ICT support staff;

3.6 ICT systems Manager/ICT support Staff

The ICT systems manager (with support staff) is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- users may only access the networks and devices through a properly enforced password protection policy;

- filtering software is applied and updated regularly and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and inform and update others as relevant;
- filtering and monitoring systems will be reviewed at least annually and in response to emerging threats, ensuring that they remain proportionate and appropriate to the needs of the school.
- that the use of the network/ internet/ Virtual Learning Environment/ remote access is frequently monitored in order that any misuse/ attempted misuse can be reported to the Headteacher for investigation/ action/ sanction.

The Governing Body and SLT must ensure that clear roles, responsibilities and effective oversight are in place for filtering and monitoring, following DfE's Filtering and Monitoring Standards. The school should identify who is responsible for approving, reviewing, and updating the filtering and monitoring systems.

3.7 **Whole school procedures linked to the use of the internet**

- The school's internet access will be designed expressly for student use and will include appropriate filtering.
- The school will ensure filtering systems are as effective as possible and are reviewed and updated regularly.
- Students taking part in video conferencing will be supervised at all times during its use.
- Formal complaints of internet misuse by students will be dealt with by the Head of student welfare.
- Any complaint about staff internet misuse must be referred to the Headteacher.
- The security of the school information systems will be reviewed regularly and virus protection will be updated regularly.
- Parents or carers will be informed of the potential use of photographs of students published on the school website and in other school publications. Parents and carers will be given the opportunity to withdraw their consent in the use of their photographs.
- Photographs on the school website and in other publications that include students will be carefully selected and will be checked to ensure the images are of an appropriate nature.
- The school will endeavour to ensure that the copying and subsequent use of internet-derived materials by staff and students complies with copyright law.
- Personal data will be recorded, processed, transferred and made available in compliance with the Data Protection Act 2018 (inclusive of the new GDPR – please see the separate data retention policy for further details).

3.8 Students

- Students will be taught what internet use is acceptable and what is not; they will be given clear objectives for internet use.
- Students will be made aware that this policy goes beyond the facilities they use in a classroom setting and that the misuse of mobile and smart technology will also constitute a breach of this policy therefore, leading to consequences decided by the Senior Leadership Team.
- Rules linked to internet access will be posted in all computer networked rooms through the Acceptable Use Policy.
- Students will be informed that internet use will be monitored.
- An online safety training programme will be delivered to all students through the ICT curriculum to raise the awareness and importance of safe and responsible use of the internet and other electronic communications tools. This programme will largely focus on ICT, PSHE and SMSC areas of learning and will include a specific focus on cyberbullying, including harassment and expressions of prejudice related to a protected characteristic (age, disability, gender reassignment, marriage & civil partnership, pregnancy or maternity, race, religion or belief, sex, or sexual orientation), responsible use of social networking and electronic communication. Learners will also be educated on extremism, radicalisation and sexual exploitation of young people, with specific relevance to the role the internet/electronic communication/social networking plays in these issues. Learners will also be made aware of the legal implications of engaging in a range of online activities, especially those involving piracy, identity theft/hacking and sexting.
- Students are advised never to give out personal details of any kind which may identify them or their location.
- Students are made aware of how to report any online safety incident or concern and are informed of both internal and external points of contact.

3.9 Teaching and support staff

- All staff will be given the school Online Safety Policy and its importance explained, including the role of the Acceptable Use Policy.
- All staff are required to be aware of the school's Data Protection and Retention Policies which are accessed via the website and school portal, with specific relevance to both the legal (The data protection act 2018) and practical importance of its application.
- If staff discover unsuitable sites, the URL, time and date must be reported to the ICT systems manager and Head of student welfare accordingly.
- Staff should be aware that internet traffic can be monitored and traced to the individual user.

- Staff will receive safeguarding and child protection (which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) updates (for example, via email, e-bulletins and staff meetings) to provide them with relevant skills and knowledge to safeguard children effectively.
- Staff will be aware that technology is a significant component in many safeguarding and wellbeing issues due to the risks posed online aswell as face to face.
- Staff will be aware that technology can facilitate, threaten and/or encourage physical abuse, sexual abuse and initiation/hazing types of violence.
- Staff will have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices, including those concerning cyberbullying, sexual exploitation, extremism, radicalisation, harassment, abuse (physical and sexual) misogynistic, self-harm and suicide
- Staff will be made aware that abuse that occurs online should not be downplayed and should be treated seriously.
- Staff will report any suspected misuse or problem to the Headteacher for investigation / action / sanction.
- All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems. *(Guidance on this can be found in the staff use of ICT policy)*
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- Staff will ensure students understand and follow the Acceptable Use Policy.
- Staff will ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Staff will 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, students should be guided to sites checked as suitable for their use by staff. Access to sites which may contain sensitive content must be reviewed by the Head of student welfare before they are approved for whole-school access.
- Staff will where appropriate, use an online safety audit tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.
- Staff are required to assess any risks and take appropriate actions to minimise harm when planning to record or livestream lessons, assembles or other activities via an online platform.
- Staff will be trained in recognising and escalating online harms, ensuring timely reporting through the appropriate internal routes.

- All staff receive annual training that includes online safety risks and how to report and respond to online harms, including emerging issues such as online misogyny and extremism.

3.10 **Parents**

- Parents will be told of the school Online Safety Policy in newsletters, the school brochure and on the school website.
- Parents /carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / Portal and information about national / local Online safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good Online 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 / portal and on-line student records*
  - *their children's personal devices in the school*
- The DSL is trained to understand the filtering and monitoring systems used, to review reports, and to escalate issues arising from online activity.

3.11 **The Prevent Duty**

In recognition of its duties under the Counter-Terrorism and Security Act 2015 to have due regard to the need to prevent people from being drawn into terrorism, and to do what it can to protect students from the risks of radicalisation and extremism, the School will:

- Provide a safe online environment by means of its filtering system as in sections 3.6 and 3.7
- Ensure students receive training on appropriate internet usage as in sections 3.8, 3.9 and 3.10
- Ensure that staff are aware of their responsibilities under the Prevent Duty and as in section 3.9
- Log internet access to assist investigations should the need arise (section 3.6 ICT Systems Manager / ICT Support Staff)
- Investigate attempts to access inappropriate online material, whether they are identified by ICT systems or staff awareness, and take suitable action (section 3.4 Head of Student Welfare)

Online safety and the school's approach will be reflected in the child protection policy and has been categorised into four areas of risk:

Content

- Being exposed to illegal, inappropriate or harmful content (e.g. pornographic, fake news, racist, misogynistic, self-harm, suicide, homophobic, expressions of religious hatred, radical and extremist.)

Contact

- Being subjected to harmful online interaction with other users. (e.g. peer-to-peer pressure, commercial advertising and adults posing as children or young adults for the purpose of grooming children.

Conduct

- Personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending, and receiving explicit images, sharing others' explicit images and online bullying)

Commerce

- risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4. Reporting of incidents

All Online safety incidents should be reported to the head of student welfare, who will log them and decide on appropriate action in conjunction with other designated persons.

5. Response to incidents

The response to a particular incident by the head of student welfare will be consistent with the whole school policy on behaviour and discipline and will have clear regard to the need for safeguarding students. Where appropriate this response may involve disclosure to external agencies.

6. **Acceptable Use Policy**

Our Acceptable Use Policy recognises that internet safety is a responsibility of the whole school community (staff, students, parents/carers). Children and young people may expose themselves to danger, whether knowingly or unknowingly, when using the internet and related technologies. Additionally, some young people may find themselves involved in activities which are inappropriate or even illegal.

The Governors recognise the school's responsibility to educate its students in the appropriate behaviours and critical thinking skills which will enable them to remain both safe and legal when using the internet and related technologies.

Droitwich Spa High School and Sixth Form Centre takes its responsibilities as a data controller and data processor seriously and are committed to using any personal data collected and held in accordance with the law. The schools policies, privacy notices and forms in relation to personal data are available for you to view on our web site at www.droitwichspahigh.worcs.sch.uk or by using the
https://website.droitwichspahigh.worcs.sch.uk/index.php/communications/information-management-and-data-protection/
The School's Data Protection Officer is the Head of Governance and can be contacted at Droitwich Spa High School and Sixth Form Centre, Briar Mill, Droitwich, WR9 0AA or by email at privacy@droitwichspahigh.worcs.sch.uk

ANNEX 1

Acceptable Use Policy for students and staff

In using the school's computers and the internet you agree to the following:

- You must not tell anyone your Username or Password (or allow anyone to use the computer system using your credentials)
- You must only access websites which are appropriate to the work you are doing at the time or websites which you have been requested to access.
- You must not attempt to bypass any network/internet security or filtering systems.
- You must not attempt to connect any personal equipment to the school network. (Staff may connect laptops to projectors and interactive boards.)

Students must also agree to the following:

- You must not access any Social networking websites or online chat rooms.
- You must never become involved in any instance of cyber-bullying
- Make sure all the messages or emails that I send are respectful and sensible
- Please show or tell a responsible adult straight away if:
    - You receive a nasty message or email or
    - You receive anything that makes me feel uncomfortable
    - You become aware of an Online safety issue affecting another person
- Always keep your personal details private and never share the personal details of any other person at Droitwich Spa High School. (This includes names, addresses, email etc.)
- You must never deliberately browse, download, upload, forward or store material (this includes files and applications) which could be considered offensive, illegal or inappropriate.
- You must ensure your online activity, both in school and outside of school, will not cause the School, staff, pupils or others any upset, embarrassment or harm at any time.
- Your use of the internet, network and portal can be monitored and logged for your own safety and the safety of others.

Failure to comply with our acceptable use policy will result in one or more of the following:

- A ban, temporary or permanent, of the use of computer facilities.
- Parents (and where considered necessary, the police) being informed of a breach of this policy and/or the law.
- Appropriate sanctions being imposed by Senior members of staff.
- Any other action which is decided by the Head teacher and Governors of Droitwich Spa High School (Including temporary or permanent exclusion).