REPTON

Online Safety Policy

Updated: Michaelmas 2023
Update by: SJL

Linked documents: Staff Employment Handbook, Safeguarding Children and Child Protection Policy, Data Protection Policy, Wellbeing Policy, IT Acceptable Use Policy, Anti-Bullying Policy, PSHE and RSE Policy, Supervision Policy, Pupil Behaviour Management Policy, Equality, Diversity and Inclusion Policy, Health and Safety Policy Statement, The School Rules, Exclusion, Removal and Review Policy, Visitors and Visiting Speakers Policy, Keeping Children Safe in Education (DfE, 2023), Prevent duty guidance for England and Wales (Home Office, 2020), Searching, screening and confiscation: advice for schools (DfE, 2018), Preventing and tackling bullying (DfE, 2017), Sharing nudes and semi-nudes (DfE, 2020), Channel duty guidance (Home Office, 2020), Relationships, Education, Relationships and Sex Education and Health Education guidance (DfE, 2019), Teaching online safety in school (DfE, 2019), Harmful online challenges and online hoaxes (DfE, 2021).

Repton · Derbyshire · DE65 6FH
Charity number: 1093166 Company number: 04390219

Contents

Key Staff

Staff Name	Responsibility
Sally Lees	Deputy Head Safeguarding, DSL
Neil Lowther	Director of Safeguarding Compliance
John Golding	Principal Deputy Head
Tom Naylor	Deputy Head Pastoral, Lead Deputy DSL
Mark Semmence	Headmaster
Sally Wan	Liaison Governor for Safeguarding
Mat Shepherd	Digital Development Manager
James Wilton	Director of Digital Development
Anna Parish	Deputy Head Inclusion and Wellbeing
Ashley Currie	Deputy Head Academic
Guy Ralphs	Interim COO (Chief Operating Officer)

1. Aims

1.1 The aim of this policy is to ensure that pupils are safeguarded by an effective online safety strategy which:

1.1.1. identifies online threats to the school community and protects staff and pupils from encountering any harmful or illegal material;

1.1.2. provides education to the school community so that they can access and use digital technology responsibly and safely;

1.1.3. will outline effective methods to identify unsafe or potentially unsafe incidents and escalate them appropriately;

1.1.4. will promote a safe, inclusive and equitable online culture across the school community.

2. Key policy responsibilities

2.1 The Deputy Head Safeguarding (and DSL) is responsible for updating the Online Safety Policy and ensuring that it complies with regulations. This member of staff is the school lead in all matters pertaining to online safety.

2.2 The Digital Development Manager, Deputy Head Safeguarding (and DSL), Deputy Head Pastoral and Principal Deputy Head are responsible for monitoring the implementation of the policy and maintaining appropriate records and risk assessments. These staff will also determine what actions, if any need to be taken.

2.3 The Deputy Head Pastoral and the Deputy Head Wellbeing and Inclusion are responsible for harvesting pupil voice in matters relating to online safety. The Deputy Head Safeguarding is responsible for incorporating pupil voice into the Pupil Safeguarding Policy.

2.4 The policy will be reviewed annually by the Governing Body.

3. Staff responsibilities

3.1 The Designated Safeguarding Lead (DSL)

3.1.1 has the lead responsibility for online safety as part of their lead responsibility for safeguarding and child protection;

3.1.2 will manage safeguarding incidents involving digital technology in the same manner as all other safeguarding matters and will log appropriately;

3.1.3 regularly monitor the logs of incidents involving use of technology that are kept by the Deputy Head Pastoral in the bullying log or in Wellbeing Manager;

3.1.4 will regularly check the monitoring and filtering online activity reports that are held in Securly;

3.1.5 will ensure that all staff receive training (including new staff induction) in the safe use of digital technology and that they understand their roles and responsibilities in relation to filtering and monitoring so that they can help protect pupils from online dangers;

3.1.6 will ensure that ensuring that all staff have appropriate data protection training at regular intervals;

3.1.7 will ensure that the staff training includes this policy, the IT Acceptable Use Policy, the Staff Employment Handbook, safeguarding information regarding the sharing of nudes and semi-nudes via image or video, cyberbullying, radicalisation and dealing with harmful online challenges or hoaxes.

3.2 The Digital Development Manager

3.2.1 is responsible for (with our ICT partners, EE)

3.2.1.1 monitoring the use of digital technology across the school and suggesting developments that can be used to better ensure the online safety of pupils;

3.2.1.2 ensuring that the school's digital infrastructure is secure and not open to malicious attack, so far as is reasonably practicable;

3.2.1.3 ensuring that only authenticated users can access the school's technology and networks;

3.2.1.4 monitoring systems and software to ensure that they are up to date and that they allow appropriate staff to monitor use of the internet, emails and Teams;

3.2.1.5 keeping logs of the above which can be referred to by the safeguarding team;

3.2.1.6 briefing the Director of Facilities on the functionality, effectiveness and suitability of all digital technology within the school which includes the filtering and monitoring systems that are in place;

3.2.1.7 escalate any safeguarding concerns raised by the above, to the DSL;

3.2.1.8 the school's filtering processes are in place, are applied and are updated on a regular basis;

3.2.1.9 the risks of circumvention of the safeguards outlined in this policy are minimised as much as is reasonably possible;

3.2.1.10 use of the school's technology is monitored to ensure compliance with this policy and that logs of suspected misuse are available to the appropriate staff so that it can be investigated via Wellbeing Manager;

3.2.1.11 the school's filtering and monitoring is working effectively in preventing the community from accessing any materials that pose a risk to the safeguarding of pupils. This includes any terrorist and extremist content.

3.3 All staff

3.3.1 should be positive role models for pupils with regards to online safety and should actively share their knowledge of online safety when appropriate;

3.3.2 should understand roles and responsibilities with relation to online safety and, filtering and monitoring specifically;

3.3.3 should abide by the IT Acceptable Use Policy when using digital technology;

3.3.4 should report any instances of educational valuable materials being blocked by the school's filtering and monitoring processes;

3.3.5 should report any concern about a pupil's online safety to the DSL.

3.4 All parents

3.4.1 should promote safe use of digital technology when pupils are online;
3.4.2 discuss safe usage of the internet, digital devices (such as mobile phones), social media and other online platforms with their children;
3.4.3 discuss suitable adults for children to speak to if they are concerned about their online wellbeing, online safety or about the online safety of another pupil;
3.4.4 should contact the DSL if they have any queries or concerns about online safety.

3.5 All pupils

3.5.1 should read the IT Acceptable Use Policy and ask if they have any queries or concerns;
3.5.2 should understand how online safety fits into the pupil safeguarding policy;
3.5.3 are encouraged to contact a trusted adult if they have any queries or concerns about online safety.

4. Filtering and monitoring

4.1 Filtering and monitoring are key tools in ensuring the online safety of the school community and the following measures are in place to ensure that our filtering and monitoring processes are robust:
4.1.1 security reports are generated weekly, including information from the school's firewall. Any concerns are escalated to the COO and other appropriate senior staff. Systems are in place to notify our IT partner of any intrusion attempts immediately.
4.1.2 controls are in place to prevent all access to any inappropriate content including pornography, self-harm, drugs, weaponry and radicalisation;
4.1.3 phishing prevention and spam filtering are also in place to protect staff and pupils from harmful or inappropriate content. Regular exercises take place to test staff awareness of these measures;
4.1.4 other controls are in place to ensure that school networks and community devices are protected from malware, ransomware, spyware and other types of harmful software as much as is reasonably possible.
4.1.5 the DSL will monitor logs to ensure that risky behaviours including age related risky online behaviours are dealt with appropriately;
4.1.6 staff and pupils are aware of what categories of content are appropriate and what categories are inappropriate via the IT Acceptable Use Policy and the Staff Employment Handbook;
4.1.7 staff and pupils have access to specific WiFi networks and the have unique login credentials which they should not share;
4.1.8 staff and pupils have IT inductions when they join the school and staff are required to complete ongoing CPD with regard to online safety, including filtering and monitoring;
4.1.9 digital literacy is incorporated into the curriculum of academic departments and online safety is taught in the PSHE curriculum in an age appropriate way;

4.1.10 pupil usage of the internet is used in a pastoral context to enable educational discussions to take place aimed at enabling pupils to make safe decisions online.

4.2 Staff and pupils have a responsibility to flag any occurrences when the filtering and monitoring procedures prevent access to necessary educational content. The community is trained to submit tickets with all necessary information to allow permitted content to be removed from the list of blocked websites.

5. Access to digital technology

5.1 The school provides internet access and access to the full Office 365 package inclusive of SharePoint intranet, Teams and email. Access is permitted on the basis of compliance with the IT Acceptable Use Policy. This use is monitored by EE in liaison with the Digital Development Manager.

5.2 Unique login credentials are required to access any of the school's WiFi networks. Any member of the school community who thinks their login credentials have been compromised must contact the Digital Development Manager and the EE helpdesk immediately.

5.3 Activity on the school network is secured to prevent malicious or accidental damage to systems or access to data. Monitoring is in place to notify our IT provider of any attempts at such activity and this is reported in the monthly service review.

5.4 The school has a separate WiFi network for guests and staff accommodation and this password is available upon request from The Lodge and is changed regularly.

5.5 The school's filtering and monitoring processes will protect pupils when using the internet and this includes access to social media, when using the school's networks. However, mobile devices with mobile data will allow pupils unrestricted access to the internet.

5.6 The school regulates mobile device usage for pupils. Staff are required to abide by the IT Acceptable Use Policy when using mobile devices.

5.7 All online policies apply to pupils and staff both on and off the school site and any misuse of digital technologies online will be investigated appropriately.

6. Misuse of IT

6.1 **Misuse by pupils:**

6.1.1 All members of the school community are required to report instances of online misuse as set out in this policy and the other safeguarding and behaviour policies. This includes pupils, staff and parents.

6.1.2 Any concerns about the misuse of online technology should be reported to the DSL and the Deputy Head Pastoral so that it can be investigated and dealt with appropriately. Any concern should also be logged in Wellbeing Manager under the appropriate heading. The DSL and the Deputy Head Pastoral will deal work together to ensure that safeguarding, wellbeing and behavioural issues are dealt with appropriately.

6.1.3 Any concern that relates to the safety of a pupil has a duty to report this immediately to the DSL in accordance with school policy.

6.2 Misuse by staff:

6.2.1 If staff have a concern about the misuse of online technology, they should report this in accordance with the whistleblowing section of the Staff Employment Handbook.
6.2.2 If staff have a concern that relates to safeguarding via staff misuse of online technology, they should report this immediately to the DSL and the Principal Deputy Head so that this can be investigated in accordance with school policy.

6.3 Misuse by miscellaneous users:

6.3.1 Anyone who has a concern about the misuse of online technology should report it immediately to the DSL.
6.3.2 The school will refer any individual whom it deems may be vulnerable to radicalisation to the Channel programme. This is so that early support can be put in place to prevent vulnerable individuals from being drawn into terrorism or terrorism related activities. Any individual who has a concern relating to extremism can refer this directly to the Police.
6.3.3 The school has the right to withdraw access to its networks at any time.
6.3.4 The school will report any suspected illegal activity to the Police.

7. Use of technology in the curriculum

7.1 As part of the tutoring and PSHE programmes pupils are educated in an age-appropriate manner in:
7.1.1 the safe use of technology. This is done in academic departments and in the PSHE programme via the tutor and external providers. This includes the use of mobile technology, social media and other software;
7.1.2 the need to be critical of all content that they come across online and are taught to seek validation of online information or opinion;
7.1.3 the definition of cyber bullying (also referenced in the pupil safeguarding policy) and how it can impact victims;
7.1.4 the need to treat others online with respect and the negative impact of harmful online behaviour;
7.1.5 how they should respond to unsafe online hoaxes and challenges;
7.1.6 how they can recognise extreme or unsafe behaviour online;
7.1.7 how they can protect themselves online and the associated privacy tools that are available.
7.2 All pupils will read and understand the IT Acceptable Use Policy every year with their tutor. Parents sign the policy on their child's behalf. The IT Acceptable Use Policy sets out the school rules for safe online behaviour and includes reference to usage of various devices; this can also be found in the School Rules.

7.3 This part of the curriculum is reviewed on a yearly basis.

8. Record keeping and risk assessment

8.1 The DSL will carry out risk assessments where a concern about a pupil's safety has been identified and appropriate action will be taken.
8.2 Risk assessment will be individualised and systematic in accordance with the school's policies.
8.3 All records are kept by the individuals listed in this policy and all incidents involving online safety will be logged in Wellbeing Manager.
8.4 All records will comply with the school's wider data protection policies.

9. Useful online resources

9.1 Useful resources for staff

9.1.1 Keeping children safe in education - GOV.UK (www.gov.uk)
9.1.2 Homepage - UK Safer Internet Centre
9.1.3 Keeping children safe online | NSPCC
9.1.4 The Prevent duty: safeguarding learners vulnerable to radicalisation - GOV.UK (www.gov.uk)
9.1.5 Channel and Prevent Multi-Agency Panel (PMAP) guidance - GOV.UK (www.gov.uk)
9.1.6 Harmful online challenges and online hoaxes - GOV.UK (www.gov.uk)
9.1.7 Eliminating Child Sexual Abuse Online – Internet Watch Foundation (iwf.org.uk)
9.1.8 The use of social media for online radicalisation - GOV.UK (www.gov.uk)
9.1.9 Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)
9.1.10 Myth vs Reality: PSHE toolkit | Childnet
9.1.11 Preventing bullying - GOV.UK (www.gov.uk)

9.2 Useful resources for parents

9.2.1 Online Safety Policy - Repton School Policies
9.2.2 Parents and Carers Toolkit | Childnet
9.2.3 Information, Advice and Support to Keep Children Safe Online (internetmatters.org)
9.2.4 Keeping children safe online | NSPCC

9.3 Useful resources for pupils

9.3.1 CEOP Education (thinkuknow.co.uk)
9.3.2 CEOP Safety Centre
9.3.3 [Withdrawn] Indecent images of children: guidance for young people - GOV.UK (www.gov.uk)
9.3.4 Children and young people - UK Safer Internet Centre

10. Review and monitoring

10.1 This policy is reviewed on an annual basis and is updated in accordance with changes to guidance and developments in best practice using the listed sources of information. This policy is monitored by the Pastoral and Safeguarding Committee.