The Crossley Heath School

Savile Park, Halifax, West Yorkshire HX3 0HG

Tel: 01422 360272 • Fax: 349099 • email: admin@crossleyheath.org.uk

E-safety Policy

November 2018

THE CROSSLEY HEATH SCHOOL

REVIEW DATE : November 2019

Version Control

Version Number	Purpose/Change	Author	Date
1	Original Policy for review	Jonathan Lees	October 2018
2	New Policy / Approved	Jonathan Lees / Frances Millington	November 2018

Table of Contents

THE CROSSLEY HEATH SCHOOL

E-safety Policy

Created:	**November 2018**
Review Date:	**November 2019**
Responsibility:	**E-safety Lead**

Statement of Intent

The Crossley Heath School e-safety policy aims to create an environment where students, staff, parents and governors and the wider school community work together to inform each other of ways to use the internet and electronic devices responsibly, safely and positively.

Outcome

- All students feel safe at school and at all alternative provision placements. They understand what constitutes unsafe situations and are aware of how to keep themselves and others safe.
- All staff understand e-safety issues are a priority.
- Training in e-safety is audited and provided to all staff
- All know how to report concerns
- Clear and transparent procedures exist for monitoring, logging, reporting incidents, evaluating, improving and measuring the impact of e-safety.

This policy will be implemented in conjunction with the following other school policies:

- Child Protection and Safeguarding Policy
- Code of Conduct
- Anti-bullying Policy
- IT Security Policy
- Mobile Phones Policy
- Acceptable Use Policy

1. Introduction

1.1. The Crossley Heath School recognises the internet and other digital technologies provide a vast opportunity for children and young people to learn. More than any other mode of technology, the Internet and digital technologies allow all those involved in the education of children and young people to promote creativity, stimulate awareness and enhance learning.

1.2. Hand in hand with the school's desire for its children and young people to access every opportunity for learning, there will be the need to keep them safe from the perils of the Internet, digital and mobile technologies. With this in mind, the school has created a policy that is aimed at developing not only a whole school approach to e-safety, but also an approach that seeks to protect children and young people who access the Internet and digital technologies outside the school environment through education for safe use. We see this as a shared responsibility.

1.3 The Crossley Heath School, as part of this policy, holds steadfast to the ethos that there should be an equitable learning experience for all students using ICT technology. We recognise that ICT can allow disabled children and young people increased access to the curriculum and other aspects related to learning.

1.4 The Crossley Heath School is committed to ensuring that all children will be able to use existing, as well as up and coming technologies safely. We are also committed to ensuring that all those who work with children and young people; as well as their parents, are educated as to the dangers that exist so that they can take an active part in safeguarding children and young people.

1.5 We believe there are many benefits of the internet, including:

- Ability to research information
- Connecting interactively with others and learning collaboratively (students and staff)
- Being taught using up to date motivating and stimulating resources
- Being able to publish instantly
- Being able to communicate quickly and easily including for sharing good practice

We want to provide information, experience and confidence to students to make them safer users of technology in a fast developing world.

1.6 We recognize that many young people are connected to others through media most, if not all their waking hours and that as a result, occurrences out of school can affect can affect their time in school for good or otherwise and that the school in partnership with families, has a joint responsibility to act on incidents that could endanger a student or cause serious distress.

2. Scope of the Policy

2.1 The Crossley Heath School will seek to ensure that the following elements will be in place as part of its safeguarding responsibilities to children and young people:

- A list of authorised person(s) dealing with child protection issues and e-safety.
- A range of policies including Safeguarding Policy, Anti-Bullying Policy, Code of Conduct, Acceptable Usage Policy and IT Security Policy that are frequently shared, reviewed and updated.
- Information to parents that highlights safe practice when using the Internet and other digital technologies in school and at home; including school staff available at key times to easily seek information and guidance.
- Adequate training for staff and volunteers.
- Adequate supervision of children and young people when using the Internet and digital technologies.
- Education of children and young people about how to use the Internet and digital technologies safely.
- A reporting procedure for abuse and misuse by children, young people and adults.

2.2 To recognise the dangers on the Internet:

Content:

- Exposure of illegal inappropriate content e.g. pornography/ignoring age ratings on games
- Lifestyle sites e.g. pro-anorexia, self-harm/suicide sites
- Hate sites
- Validation of content difficulties i.e. authenticity/accuracy
- Content / Interaction
- Grooming
- Cyber-bullying in all its forms
- Identity theft

Conduct:

- Digital tattoo (footprint) and online reputation
- Health and well-being e.g. time spent gaming
- Sexting
- Copyright
- Privacy issues

2.3 To promote discussion and systematic development of knowledge and positive behaviour, leading to safer internet usage year on year, with a measurable impact on e-safety. It is intended that the positive impact of the policy will be seen online and offline, in school and at home; and ultimately beyond school and into the workplace.

2.4 The Crossley Heath School Academy Trust will rely on DfE and ICO guidance and documentation with regard to data protection, data storage and privacy compliance.

3. Policies and Practices

3.1 Acceptable Use Policy (AUP) for all staff, governors and external contractors

Terms of agreement are read and signed for, agreeing standards and expectation relating to usage in order to promote and secure good behaviour.

3.1.1 This policy aims to ensure that the internet, email and other technologies are used effectively for their intended educational and recreational purposes, without infringing legal requirements or creating unnecessary risk (in a safe and secure way).

3.1.2 The Crossley Heath School Academy Trust recognizes that in certain planned curricular activities, access to otherwise considered inappropriate sites may be beneficial for education use. In such circumstances, such access should be pre-planned and recorded and also permission given by senior leaders, so that the action can be justified, if queries are raised later.

The school maintains and regularly monitors a web filtering system recognising that no system is perfect and young people will often seek to get around the filters.

3.1.3 Incidents which appear to involve deliberate access to websites, social media groups, newsgroups and any other online groups that contain the following material will be reported to the Designated Leader for Child Protection or in the case of staff or volunteers the Head Teacher.

- Indecent images inclusive of abuse (images of children whether they are digital or cartoons, apparently under the age of 16 years old, involved in sexual activity or posed to be sexually provocative)
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material or anti-religious material
- Violence and bomb making
- Illegal taking or promotion of drugs
- Software piracy
- Any criminal activity
- Anything which alerts under “Prevent” to suggest a danger of radicalisation or extremism.

3.2 IT Security Policy

Terms of agreement are read and signed for, agreeing standards and expectation relating to usage in order to promote and secure good behaviour.

3.2.1 This policy aims to protect, preserve and manage the confidentiality, integrity and availability of school IT assets.

3.2.2 It ensures that staff are aware of their own responsibilities for complying with relevant legislation.

3.2.3 It ensures that staff understand the need for information and IT security and their own responsibilities in this respect.

3.3 Child Protection and Safeguarding Policy

3.3.1 This policy aims to safeguard and promote students' welfare, safety and health by fostering an honest, open, caring and supportive climate with students' welfare as paramount importance.

3.3.2 It lays out the school's commitment, structure, roles and responsibilities for all procedures and training which include the reporting of all concerns e.g. neglect / at risk of sexual exploitation / at risk of abuse through female genital mutilation / at risk of radicalisation and online grooming / physical abuse / emotional abuse / sexual abuse.

3.3.3 It makes clear adherence to all required legislation and guidance and is overt in recognising dates of training, record keeping, monitoring and quality assurance.

3.3.4 It recognises the importance of updates, training and awareness regularly and as required not just every 2-3 years to ensure all staff can spot signs of potential abuse / neglect / risk of exclusion / risk of radicalisation etc.

3.4 Anti-Bullying Policy

3.4.1 This policy seeks to prevent and reduce bullying conducted by any means including verbal, physical, emotional and cyber.

3.4.2 It makes clear to all stakeholders their rights and responsibilities.

3.5 Code of Conduct

3.5.1 Lays out the code of behaviour/conduct expected of staff both paid or volunteers.

3.4.2 Includes "Guidance for safer working practices for those working with children and young people in education settings October 2015".

3.4.3 The above guidance can be found in the "Staff Handbook" and in the Policies folder on Staff Public.

4. Reporting Abuse

4.1 There will be occasions when either a student or an adult within the school, receives an abusive email or accidently accesses a website that contains abusive material. When such a situation occurs, the expectation is that the child, young person or adult should report the incident immediately.

4.2 The Crossley Heath School also recognises that there will be occasions where children and young people will be the victims of inappropriate behaviour that could lead to possible or actual significant harm, in such circumstances safeguarding procedures should be followed. The expected response will be to take the reporting of such incidents seriously.

4.3 The Designated Safety Lead as part of their safeguarding duties and responsibilities will, assist and provide information and advice in support of child protection enquiries and criminal investigations.

4.4 The school website has a link to CEOP and students are taught to use the button appropriately and who to go to for reporting concerns.

5. Education and Training

5.1 The Crossley Heath School is committed to harnessing the power of the Internet and other digital technologies to transform the learning of children and young people. We are also dedicated to ensuring that children and young people have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the Internet and other digital technologies safely.

5.2 As part of the achieving the above, the school will seek to ensure that e-safety training takes place regularly for adults that teach, supervise students, manage and/or support the school e.g. network managers and technicians.

5.3 The curriculum we provide to students to use electronic technologies safely now and in the future and is varied and widespread, i.e. Students are taught to assess and manage risks. They are taught in a variety of environments across all years.

e.g. - In computing classes with experienced teachers
- In Life Skills and with their mentor
- In assemblies

5.4 Information for parents/carers is provided through our website, displays on parent evenings and occasional special events for parents.

6. Infrastructure and Technology

See “IT Security Policy”

7. Provision / Curriculum

Activity / Provision	Details	Year Group
Agreement	Parents and student's agreement Parents tick box on data form on entry and both parents and students sign the agreement at the start of each year	All years
ICT expectations and safety briefing session includes how to report concerns / incidents	New starters Year 7, first computing lessons New starters Year 12	Year 7 Year 12
Bullying / Cyber Bullying	Cyber-bullying covered in PHSE lessons. Cyber-bullying covered in Computing lessons Anti-bullying week (Nov)	Years 7 & 8 Years 7 & 8 All Years
E-safety / CEOP / Sexting	E-Safety, Sexting and CEOP covered in Computing lessons and assemblies Sexting covered in PHSE days and assemblies Safer Internet Day	Years 7 & 8 Year 9 & 10 All years
Personal Safety / Assessing and Minimising risk / CSE / Grooming	Grooming, Personal Safety, Minimising risk covered in Computing lessons Grooming covered in PHSE days and PSE lessons	Year 7 & 8 Years 9, 10, 12 and 13
Anti-Radicalisation / Preventing Extremism	Anti-radicalisation covered citizenship and PSE lessons Prevent covered in citizenship and PSE lessons	Year 9, 12 and 13 Year 9, 12 and 13
Issues raised as a concern by students	Discussions with Pastoral Leaders, form tutors and wellbeing Counsellor	All years

8. Monitoring and Evaluation

8.1 The first responsibility for monitoring the use of the internet and digital technologies lies with the staff. These should include both physical observation (supervision of use by an adult, where appropriate) and technical monitoring.

8.2 The IT Support team, through the system monitors and audits of the use of the Internet and email to see whether users are complying with the policy, and is able to investigate in detail where there are concerns.

8.3 Behaviour, attitudes, well-being and development are examined regularly in learning walks, observations, drop-ins and SLT reviews.

8.4 The policy will be reviewed annually or promptly upon:

- Serious and/or frequent breaches of the Acceptable Use Policy
- Serious E-safety incidents
- New guidance from the DfE
- Significant changes in technology
- Serious E-safety incidents in the community affecting students
- Advice from the Police

9. Inappropriate Use and Sanctions

9.1 Where there is an inappropriate or illegal use of the Internet and digital technologies, the following sanctions will apply:

Child / Young Person:

- The child / young person will be disciplined according to the behaviour policy of the school which will include informing parents, detentions, and the use of Internet and email being withdrawn. Incidents are logged in PARS and dealt with by the Pastoral Leaders or SLT team. Exclusion will be used as a last resort.

- Serious Breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

Adult (Staff and Volunteers)

- The adult may be subject to the disciplinary procedure process of the school, if it is deemed he/she has breached the E-Safety, IT Security or Acceptable Use policy.

- Serious breaches may lead to the incident being reported to the Police or other regulatory bodies, for instance, illegal Internet use or child protection concerns.

9.2 If inappropriate material is accessed, users are required to immediately report this to Jonathan Lees who will then inform the IT Support team and the DSL if necessary.

10. Working with Families / other partners / agencies

10.1 All related policies are available on the school's website and on paper on request.

10.2 A newsletter is emailed to parents with information and updates at least twice per year.

10.3 E-safety issues and allegations of cyber-bullying are investigated and dealt with by care and guidance by staff involving parents throughout if necessary.

10.4 Where children are deemed at risk the DSL follows safeguarding procedures and will keep families informed as much as possible by phone, email or school visit.

10.5 Information on e-safety is posted on the school website for families and students to refer to in and out of school.

10.6 A contact and email address is available for parents/carers to raise concerns and ask for guidance and support related to e-safety issues.

Appendix A / Roles

The School E-safety Lead / Jonathan Lees:

- The Crossley Heath School has a designated e-safety lead who reports to the Designated Safeguarding Lead(DSL), Governors and coordinates e-safety provision across the school.
- The e-safety lead is responsible for auditing, monitoring, review and the evaluation of this policy.
- The e-safety lead coordinates audits, feedback and provides training for staff and governors ensuring that all are aware of their responsibilities and the schools e-safety procedures. The lead is also the first port of call for staff requiring advice on e-safety matters.
- Although all staff are responsible for upholding the e-safety policy and safer Internet practice, the e-safety lead and DSL are responsible for monitoring Internet usage by students and staff on school machines and mobile devices connected to the BYOD WIFI network.
- The e-safety lead is responsible for promoting best practice in e-safety within the wider school community, including providing and being a source of information for parents.

The Designated Safeguarding Lead / Jonathan Brownlie:

- The Crossley Heath School has a fully trained designated Safeguarding Lead(DSL) who reports to the Head Teacher and Governors and coordinates safeguarding provision across the school.
- The DSL receives all reports of potential and actual breach of code of conduct related to e-safety and where necessary will inform the Head Teacher.
- The DSL must be able to differentiate which e-safety incidents are required to be reported to CEOP, local police, LADO (Head Teacher referred), social services and parents/guardians; and also determine whether the information from such an incident should be restricted to nominated members of SLT.
- The DSL is responsible for monitoring Internet usage by students and staff alongside the e-safety lead.

Governors responsibility for e-safety:

- At least one Governor is responsible for e-safety, and the school e-safety lead or DSL will liaise directly with the Governor with regards to reports on e-safety effectiveness, incidents, monitoring, evaluation and development and maintaining links with local stakeholders and the wider school community.
- They provide and evidence a link between the school, Governors and parents.
- An audit of Governor IT competence, relevant outside experience and qualifications is established by the designated governor to identify training needs and create a schedule of training as required. It is essential that the Governor tasked with overseeing and monitoring e-safety has demonstrable experience, skills or qualifications to match the role.

The IT Support Team:

- The IT Support Team are responsible for maintaining the schools network and IT infrastructure. They need to be aware of current trends in IT security and ensure the schools system and access to the Internet is secure. They need to further ensure that all reasonable steps have been taken to ensure that systems are not open to abuse or unauthorised external access.
- The IT Support Team need to maintain and enforce the school's IT Security policy, guidelines within the Acceptable Use Policy and maintain Internet filtering.

Teaching Staff and Pastoral Leaders:

- When students report e-safety concerns, teaching staff must take this seriously, record the incident and refer it to the appropriate person:
  a) Safeguarding or at risk of radicalisation/extremism > DSL
  b) Cyber-bullying / General Concern > Pastoral Leaders
  c) Misuse of IT usage agreement > Pastoral Leaders
- Pastoral Leaders and staff that teach e-safety in the curriculum must have a higher level of training in e-safety and regular updates.

All Staff (including Teachers and Pastoral Leaders):

- All staff must be aware of the current school e-safety policy, practices and associated procedures for reporting e-safety incidents.
- All teaching staff will be provided with basic e-safety training and regular updates at least once per year.
- Non-teaching staff can be provided with e-safety training if it would be useful but is not mandatory.
- When using IT facilities all teaching staff need to monitor student Internet and computer usage in line with the Acceptable Use Policy. This also includes the use of personal technology such as iPads, phones and other gadgets.
- Any incidents of exposure of illegal inappropriate content e.g. pornography must be reported immediately to the e-safety lead.
- All staff must be aware of the actions to take in the event of misuse or potential/actual breach of conduct.

Students:

- Are required to use school Internet and computer systems in agreement with the terms specified in the "ICT Code of Practice" which can be found in their planner.
- Students must be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the CEOP report abuse button.
- Students have to be aware that school agreements cover all computer, Internet and gadget usage in school, including the use of personal items such as phones whilst in school.

- Students need to be aware that their Internet use out of school on social media sites is covered under the agreements if it impacts the school and/or its staff and students in terms of cyber-bullying, reputation or illegal activities.

Parents and Carers:

- It is hoped that parents and guardians will support the school's stance on promoting good Internet behaviour and responsible use of IT equipment both at school and at home.
- The Crossley Heath School expects parents and carers to sign the school's agreements, regarding their child's use and also their own use with regard to parental access to school systems such as websites, social media, online reporting, arrangements and questionnaires.
- The school will provide opportunities to educate parents with regards to e-safety.

Other Users:

- Other users such as school visitors, or wider school community stakeholders or external contractors will be given a specific level of access and usage when required.

Appendix B / Actions to take in the event of misuse or potential/actual breach of conduct

1. Illegal Material

If you find illegal material on the school network, or log evidence to suggest that illegal material has been accessed on the Internet:

If the illegal material is (or suspected to be):

a) Child sexual abuse images
b) A non-photographic child sexual abuse images
c) Or a criminally obscene adult content

Report the finding immediately to the DSL or the Head Teacher. DSL or Head Teacher to contact the Police and report to the IWF (Internet Watch Foundation) - https://report.iwf.org.uk/en/report.

If the Head Teacher or DSL are unavailable, contact the local Police.

Do NOT copy, archive, forward, send or print out the image(s).

If there is a child protection issues:
Follow the school's child protection procedures and contact the DSL.

If you find material on the school network or Internet which involves grooming or suspected child abuse:

Report the finding immediately to the DSL or the Head Teacher. DSL or Head Teacher to contact the Police and report to the IWF (Internet Watch Foundation) - https://report.iwf.org.uk/en/report.

If the Head Teacher or DSL are unavailable, contact the local Police.

2. How to deal with e-safety incidents:

Staff and Student / Illegal activities:

- Report to the Head Teacher or Deputy Head
- The local Police to be contacted. Child Protection procedures take precedence over AUPs if CP is a factor.
- IT support should be contacted to obtain further evidence.
- Incident log passed to e-safety lead.

Student using the Internet in lessons not relevant to the lesson

- Class teacher to deal with the issue and write up an incident submitted to Pastoral team if needed.
- Student may receive a warning and if more serious can be banned from using the Internet for a period.

Staff excessive use of the Internet during work time (including social media)

- Concerns should be raised with and dealt by line manager.
- If issue continues, the Head Teacher can be informed and it may be a disciplinary matter.

Bypassing the school's filtering system

- IT Support should be contacted to obtain further evidence.
- Student: The class teacher or Pastoral leader will deal with the matter and write up an incident log and pass to e-Safety Lead.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

Viewing pornographic material

- IT Support should be contacted to obtain further evidence.
- Student: A serious matter to be dealt with by the SLT on duty. Write up an incident log and pass to e-Head Teacher and Safety Lead. Parents/carers will be informed and the student will be banned from the using the Internet for a period.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.
- The Police must be contacted if indecent and illegal material was accessed.

Using a mobile phone or other digital device in lesson without teacher agreement

- The Class teacher will deal with the matter and arrange for the device to be confiscated. This will be named and stored securely in the school office until the end of the day and a message will be sent to the parent.

Cyber-bullying

- IT Support should be contacted to obtain further evidence.
- Student: The person who this is reported to will fill out an incident sheet and pass it on to the Pastoral Leaders who will decide whether it can be dealt with by them or if it is more serious and needs to go to SLT or the DSL. Parents/carers to be informed. Normal school sanctions apply. Incident log passed to e-safety lead.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

Writing malicious comments about the school or bringing the school name into disrepute – whether in school time or not:

- IT Support should be contacted to obtain further evidence.
- Student: The class teacher will deal with the matter and write up an incident report which needs to go to SLT. Parents/carers to be informed. Normal school sanctions apply. Incident log passed to e-safety lead.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

Sharing usernames and passwords

- IT Support should be contacted to disable the accounts.
- Student: The class teacher will deal with the matter. Normal school sanctions apply.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

Deleting someone else's work or unauthorised deletion of school files

- IT Support should be contacted to obtain further evidence.
- Student: The class teacher will deal with the matter. Normal school sanctions apply.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

Trying to hack into another person's account, school databases, school website or online fraud using the school network

- IT Support should be contacted to obtain further evidence.
- Student: A serious matter to be dealt with by the SLT on duty. Write up an incident log and pass to e-Head Teacher and Safety Lead. Parents/carers will be informed and the student will be banned from the using the Internet for a period.
- Staff: The issue will be raised with the Head Teacher and will be a disciplinary matter. Incident log passed to e-safety lead.

3. E-safety and the Law

Computer Misuse Act 1990, sections 1-3
GDPR / Data Protection Act 2018
Freedom of Information Act 2000
Communications Act 2003 section 1,2
Protection from Harassment Act 1997
Regulation of Investigatory Powers Act 2000
Racial and Religious Hatred Act 2006
Protection of Children Act 1978
Sexual Offences Act 2003
The Education and Inspections Act 2006 (Head Teachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site. Also, staff can confiscate mobile phones if they cause disturbances in class breaching the school behaviour policy).