Crossflatts Primary School

Online Safety Policy

Updated Summer 2020

Approved by the governing body on:	15-05-2020
To be reviewed on:	May 2022
Signed on behalf of the governing body:	*Mary Morgan*

NB. This guidance will be retained for a period of 7 years from replacement.

Crossflatts Primary School

Online Safety Policy

Version 2

Reviewed Summer 2020

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning.

Children and young people should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The E-safeguarding Committee

Richard Atkins (E-Safeguarding Leader, ICT Coordinator & Teacher)
Nicola Bennett– (Head, Designated Safeguarding Lead Person)
Claire Thirkill (Deputy Headteacher and Safeguarding Lead)
Katy MacCuish (School Business manager)
Mary Morgan (Chair of Governors – Named governor for Safeguarding)

Development and Review of this policy.

This e-safeguarding policy was approved by the *Governors School Improvement Committee*	
The implementation of this e-safety policy will be monitored by the:	*The E-safeguarding committee*
Monitoring will take place at regular intervals:	*Annually*
The E-Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	Summer 2021
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Children's services (Keighley) Bradford Learning Network

Monitoring the impact of the policy
The school will monitor the impact of the policy using

- Logs of reported incidents in the e-safeguarding incident log and on CPOMS to be monitored by HT/DHT and E-Safety Lead.
- Internal monitoring data for network activity
- Smoothwall user logs. Our technician can access these logs to see which users accessed which web sites at which times, the Bradford Learning Network can also be utilised to see this data.
- Student e-safeguarding data will be gathered through the use of the Bradford Council Children's Services eSafeguarding questionnaire available at: http://bradfordschools.net/limesurvey/ . Progress will be monitored at the start and the end of each academic year.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors School Improvement Committee receiving regular information about e-safety incidents and monitoring reports

The Governor responsible for safeguarding Mary Morgan has taken on the responsibility for e-safeguarding.

The role of this governor will include:

- regular meetings will include-safeguarding where e-safeguarding issues will be discussed
- regular monitoring of e-safety incident logs
- reporting to relevant Governors through minutes of meetings and Headteacher's Report

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safeguarding (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Leader Richard Atkins
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator / Officer and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant

- The Headteacher and E-safeguarding leader are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. This is detailed in the Child Protection & Safeguarding Policy.

E-Safeguarding Leader

- takes day to day responsibility for e-safeguarding issues and has a leading role in establishing and reviewing the school e-safeguarding policy.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- attends the Governors School Improvement Committee (which discusses e-safeguarding issues).

Network Manager / Technical staff:
Datacable, the school technician ensures:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that they keep up to date with e-safety technical information and updates the E-safeguarding leader or ICT coordinator as relevant.
- that monitoring software and anti-virus software is implemented and updated

Teaching and Support Staff
are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy
- they have read, understood and signed the school Staff Acceptable Use policy / agreement (AUP)
- they report any suspected misuse or problem to the E-Safety leader for investigation
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities. E-safeguarding lessons are taught through the Innovation Centre's E-Safety Curriculum.
- students / pupils understand and follow the school e-safety and acceptable use policy
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

Named person for child protection and safeguarding

Nicola Bennett (Head) Nina Dobson (Deputy Head) , Claire Thirkill (Deputy Head and Inclusion Manager) and are the designated Safeguarding Lead persons.

They are trained in e-safety issues and are aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Children

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use policy, which they will be expected to understand / sign before being given access to school systems.
- are aware that breaking the AUP would cause them to follow sanctions laid out in the Behaviour and Anti-Bullying policy.

Parents / Carers

The school will take every opportunity to help carers / parents to understand issues related to e-safeguarding. We will assist parents to understand key issues in the following ways:

- The school will arrange annual e-safety training and information meetings for parents
- Information and guidance will be provided for parents with advice on the use of the internet and social media at home
- Parents are asked to discuss the Pupil Acceptable Use policy with their children and are invited to sign a letter to say they have done so.

Community Users

Community users, visitors and volunteers will inform the Headteacher or Deputy Head of any web sites they wish to access. No person can log on to the internet without a user account or the Internet password. A community user account with minimal privileges will be given after discussion of the sites they wish to access.

Education – Pupils

The education of pupils in e-safety is an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and to build their resilience.
E-Safety education will be provided in the following ways:

- A planned e-safety programme is delivered as part of PHSE in the form of the The Innovation Centre's E-Safety Curriculum .
- The Bradford ICT Scheme of work also highlights e-safeguarding issues that arise in the context of ICT lessons.
- Key e-safety messages are reinforced as part of a planned programme of assemblies. They take place once a term and are mentioned in the school diary.
- Pupils are taught in all lessons to be critically aware of the material and content they access on-line and be guided to validate the accuracy of information. Validation and cross referencing of information is covered in the research strand of the Bradford ICT scheme of work.
- Rules for use of ICT systems will be posted in all rooms and displayed on log-on screens. Students will sign a class copy of the Acceptable Use policy and it will be on display in their classroom.
- For directed searches in school, staff should direct children to Primary Safe Search or other search tools recommended in the research section of the Bradford ICT Scheme of work.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet. Copyright free audio and image sources are detailed in the Multimedia and Sound strands of the Bradford ICT scheme of work which the school follows.

Education - Training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A staff meeting covering e-safeguarding will take place annually. This will be delivered by a member of Bradford Council Children's Services Curriculum ICT Team or a member of the E-safeguarding Committee.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use policies.

Education - Governor Training

Governors should take part in e-safety training / awareness sessions.

E-safeguarding training is planned annually for governors. This may be delivered by Bradford Children's Services consultants or by members of the e-safeguarding committee.

Internet Provision

The school internet is provided by the Bradford Learning Network (BLN), a DFE accredited educational internet service provider. All sites are filtered using the Smoothwall filtering system which also generates reports on user activity. The e-safe filtering and maintaining system is called e-safe.

Use of digital and video images - Photographic, Video

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images online.
- Staff are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Photographs of children published on the website or blog must not contain names.
- Only pupil's first names should be used on Twitter
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see form in appendix)

Data Protection

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly logged-off at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected memory sticks, as provided to all members of staff.

Passwords

All users (adults and children) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security

- Passwords for new users, and replacement passwords for existing users can be allocated by Data cable.
- Users will change their passwords regularly.

Members of staff will be made aware of the school's password policy:

- At induction
- Through the school's E-safeguarding policy

- Through the Acceptable Use Agreement

Pupils will be made aware of the school's password policy:

- In ICT and / or E-safeguarding lessons
- Through the Acceptable Use Agreement

All users will be provided with a username and password by Datacable, who will keep an up to date record of users and their usernames.

Prevent – Anti Radicalisation and extremism

The school is aware that vulnerable children and adults may be exposed to terrorist propaganda through social media and the internet. The school is committed to ensuring all children are safeguarded and through the implementation of the safeguarding and child protection policy, this policy incorporates E-Safety.

Our 'Forensic' Monitoring system in school monitors all key strokes and internet searches so that the school can supervise the information that the children and adults access.

Appendix A Staff Acceptable Use policy Crossflatts Primary School.

ICT Acceptable Use Agreement for Staff, Governors & Trainees

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this Acceptable Use Agreement. Members of staff should consult the school's e-Safeguarding Policy for further information and clarification.

- I understand that my use of school information systems (e.g. SIMS), Internet (including email) and any other networked ICT resources will be monitored and recorded to ensure Policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than on request from an authorised system manager (including but not limited to the ICT Coordinator/ Business Manager and external technical support provider).
- I will not install any software (including mobile apps) or hardware without permission from the ICT Coordinator.
- I will ensure that pupil data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will adhere to copyright and intellectual property laws and only publish media which I own, have permission to use or is copyright-free.
- I will report any incidents of concern regarding children's safety whilst using new technologies in or out of school to the e-Safety leader.
- I will ensure that electronic communications with pupils including blog comments and email are compatible with my professional role and that messages cannot be misunderstood or misinterpreted. I understand that befriending pupils on instant messaging services and social networking sites is prohibited.
- I will not use any personal device (including cameras and mobile phones) to capture images, videos or audio of pupils or to access social networking sites in school time.
- I will promote e-Safety with pupils in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the ICT Acceptable Use Agreement.

Name: …… Signed: …… Date: ……

Appendix B Agreement for children

Dear Parents/Carers,

As a school we are committed to safeguarding our children.

By working together schools and parents can help children achieve more. By setting out the responsibilities of the school, parents and children, we can all understand our role in helping children do their best.

Please see below a copy of the current agreement, which we invite you to read and sign. If you agree to do this, please sign and return the slip and keep your copy of the agreement. If you feel your child understands their part of the agreement they can also sign the slip below.

Acceptable use Agreement of ICT in School

- We only access the computer system with the login and password we have been given
- We will not access other people's files or use their password and login details
- We ask permission before using the internet
- We only use websites our teacher has chosen or they have approved
- We will immediately inform a teacher and hide any webpage we do not like
- We only email people our teacher has approved
- We send emails that are polite and friendly
- We will immediately report any unpleasant messages received as this will help protect other children and ourselves
- We never give out our personal information including our home address or phone number
- We never arrange to meet anyone we have met over the Internet
- We never open emails sent by people we do not know
- We will tell the teacher if we see anything on a device we are unhappy with
- We will not use mobile phones in school time unless instructed to do so by a teacher
- We understand that we are responsible for good behaviour on the Internet and when using ICT equipment and that inappropriate use may lead to access being withdrawn

Kind regards

Mrs Nicola Bennett
Headteacher

✂……

REPLY SLIP

I/We have read the Acceptable use of ICT agreement and agree to sign it.

Parents/Carers of…… Class……

Signed……

Child's signature…… Class……

Date……..

Crossflatts

PRIMARY SCHOOL