Iver Heath Junior School

Online Safety Policy

Approved by:	Governors	**Date:** September 2022
Last reviewed on:	September 2023	
Next review due by:	September 2025	

Online Safety Policy and Procedural Guidance

Online Safety Policy and Procedural Guidance

1. Introduction

Iver Heath Junior School recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and promote best practice in their social, moral, spiritual and citizenship development, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This Online Safety Policy should be read alongside other relevant school policies e.g. Child Protection & Safeguarding, Anti-Bullying, Child-on-Child Abuse and Behaviour.

Keeping Children safe in Education (2022) outlines that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: child to child 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: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and seeking out or sharing any other inappropriate or illegal materials.

commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

This policy outlines what Iver Heath Junior School will do to teach Online Safety and prevent and tackle cyber-bullying.

2. Creation, Monitoring and Review

Our Online Safety Policy has been written by the school, building on the Buckinghamshire Council e-Safety Policy and government guidance such as *Keeping Children Safe in Education 2022.* It involves all key stakeholders in the content of this policy and gives a special ear to the voice of the children at our school. It has been agreed by the senior management and approved by governors. The impact of the policy will be monitored regularly with a full review being carried out at least once a year. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

At Iver Heath Junior School we have the following policies in place that should be read in conjunction with this policy: Child Protection and Safeguarding Policy, Anti-Bullying Policy, Child-on-Child Abuse Policy and Mobile Phone policy.

3. Roles and Responsibilities

This policy applies to all members of the school community who have access to the school's IT systems. Any user of the IT systems must adhere to the Online-Safety Rules and the Code of Conduct. The Online-Safety Policy applies to all use of the internet and forms of electronic communication such as email.

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All main class-teachers are required to deliver Online-safety lessons to their classes or ensure that they are taught. When informed about an online-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have online-safety concerns and who to talk to. Where any report of an on-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Lead or Deputy may be asked to intervene with appropriate additional support from external agencies.

3.1 Headteacher:

- Both the Computing co-ordinator as Online-Safety Officer and the Headteacher as Designated Safeguarding Lead are responsible for keeping up to date with new technologies and their use, as well as attending relevant training
- Foster a culture of safeguarding where online safety is fully integrated into whole school safeguarding
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant to the Local Safeguarding Partnership
- Liaise with the Deputy Designated Safeguarding Lead on all online safety issues that might arise and receive regular updates on school issues and broader policy and practice information
- Take overall responsibility for data management and information security ensuring the school's provision follows best practice in information handling; work with the Data Protection Officer, Deputy Designated Safeguarding Lead and governors to ensure a GDPR-compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Ensure the school implements and makes effective use of appropriate ICT systems and services including school-safe filtering and monitoring, protected email systems and that all technology including cloud systems are implemented according to child-safety first principles
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff (e.g. network manager) who carry out internal technical online safety procedures
- Ensure governors are regularly updated on the nature and effectiveness of the school's
- arrangements for online safety
- Ensure the school website meets statutory requirements

3.2 Learner:

- Are responsible for using the IT systems in accordance with the ICT Acceptable Use Policy, which parents sign at the time of admission
- Must act safely and responsibly at all times when using the internet
- Attend e-safety lessons as part of the curriculum
- Must follow reporting procedures where they are worried or concerned, or where they believe an Online-safety incident has taken place involving them or another member of the school community
- Must follow the IHJS 3 golden rules during computing lessons

3.3 Staff:

- Are responsible for using IT systems in accordance with the ICT Acceptable Use Policy
- Are responsible for displaying a model example to learners at all times through embedded good practice
- All digital communications with learners must be professional at all times
- Online communication with learners is restricted to the school's online learning platforms such as Showbie and Purple Mash
- Should not use external platforms not hosted by Buckinghamshire Council, such as social media sites, to communicate with learners
- Are aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
- In addition, class teachers are responsible for monitoring pupils' use of the internet during lessons and, by regularly viewing activity logs, pupils' communication with each other whilst using our Showbie online learning platform
- Ensure that students are aware that all bullying concerns, including cyber-bullying, will be dealt with sensitively and effectively so that students feel safe to learn.

This policy will, however, be monitored and kept under review.

4. Security

The school will work with Buckinghamshire Council and Bucksgfl to ensure that systems are in place to protect pupils.
The Bucksgfl network uses Webscreen TM which is an industry-standard system designed by educators to suit the age and curriculum requirements of the pupils. If staff or pupils discover unsuitable sites, the URL must be reported to the ICT coordinator. Any material that the school believes is illegal must be reported to the appropriate agencies such as CEOP (Child Exploitation and Online Protection command).

5. Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Buckinghamshire Counil can accept liability for the material accessed, or any consequences resulting from Internet use.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

6. Behaviour

The School will ensure that all users of technologies adhere to the standard of behaviour. The school will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the behavior policy.
Where conduct is found to be unacceptable, the school will deal with the matter internally.
Where conduct is considered illegal, the school will report the matter to the police.

7. Communications

7.1 E-mail:

- Pupils may only use approved email accounts.
- Pupils must immediately tell an adult if they receive offensive email.
- Pupils must not reveal any personal details or the details of others in e-mail communication, and they must never make arrangements to meet anyone through electronic communication.

7.2 Social networking:

- Bucksgfl does not allow access to social networking sites. The school is aware that bullying can take place through social networking, especially when a space has been setup, and that others are able to view comments.
- As part of e-safety lessons pupils will be advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc. Pupils will also be advised not to publish specific and detailed private thoughts.

7.3 Video Conferencing:

Video conferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity. Equipment connected to the education broadband network should use the Adobe Connect system using staff bucksgfl usernames and passwords. Video conferencing will be supervised appropriately and parents/guardians should agree for their children to take part in video conferences as part of their Parental Consents upon starting school. Dialogue will be established with the other conference participants before taking part in a video conference. If it is a non-school site, checks will be made to ensure that they are delivering material appropriate for the learners.

7.4 Website:

- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The contact details on the website will be the school address, email and telephone number.
- Staff or pupils' personal information will not be published.
- The website will show respect for intellectual property rights and copyright. Images that include pupils will be selected carefully.

7.5 Emerging technologies:

Emerging technologies will be examined for their educational benefit and a risk assessment will be carried out before their use in school.

7.6 SHOWBIE

- Staff and pupils will ensure that any communication through the Class discussion on SHOWBIE is appropriate at all times. Any inappropriate language or behaviour will be treated seriously and in line with the behavior and anti-bullying policies.

8. Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other individual's rights (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners. Our aim is to reinforce good practice as well as to offer further information for all users on how to keep their personal information safe. Photographs of activities on the school premises will be carefully considered before publication. Permission for the use of photographs is given by parents or guardians upon admission to the school.

9. Personal Information

- Personal information is information about a particular living person. The school collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Only names of staff will appear on the school website. No personal information will be available on the website without consent.
- Staff must keep learners' personal information safe and secure at all times.
- Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.
- All teacher laptops are password protected and signed for by the member of staff concerned.
- Where the personal data is no longer required, it will be securely deleted.

10. Education and Training

- With the current unlimited nature of internet access, it is impossible for the school to eliminate all risks for staff and learners. It is our view therefore, that the school should support staff and learners in staying safe online.
- Issues associated with e-safety apply across the curriculum and learners will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.
- Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either when that material is directed to them, or where it is discovered as part of a random search.
- Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties.
- Class teachers will ensure that Online safety lessons will be taught each year.
- Children will be a part of a whole-school focus called E-Safety Week each year.

11. Cyber-bullying and Children at potential risk from unsafe online use

Online Bullying / Cyberbullying is the use of technology (social networking, messaging, text messages, e-mail, chat rooms etc.) to harass threaten or intimidate someone for the same reasons as stated above.

Online bullying can take many forms, including but not limited to:

- Abusive or threatening texts, emails or messages
- Posting abusive comments on social media sites
- Sharing humiliating videos or photos of someone else
- Stealing someone's online identity
- Spreading rumours online
- Trolling – sending menacing or upsetting messages through social networks, chatrooms or games
- Developing hate sites about another person
- Prank calls or messages
- Group bullying or exclusion online
- Anonymous messaging
- Being abusive, either individually or as a group, during on-line gaming platforms
- Encouraging a young person to self-harm
- Pressuring children to send sexual messages or engaging in sexual conversations

11.1. Children reporting Cyber bullying or concerns they have about unsafe online use

Teachers and staff members at Iver Heath Junior School build positive relationships with the children in the school. We are a small enough school for children to continue to build relationships with staff throughout their time at IHJS. Members of staff run after-school clubs, take regular assemblies, are visible on playground duties and around the school. Building relationships are encouraged and valued at our school. As such, we encourage the children to report to and involve an adult as soon as they find themselves in a situation that make them feel in any way uncomfortable.

However, we also recognise that some children may find themselves in situations where they do not, for whatever reason, feel comfortable to do that.

In such cases children may:

- Use the emotion cups in their classroom and put their lollystick into the worried/anxious cup to alert their teacher that something is wrong.
- Use the **Tell Me Box.** The Tell Me Box is located in the library with simple forms to fill in to alert staff that a child would like to report child-on-child abuse. The child can fill in their name on a slip and put it into the box. The box will be checked regularly by the Deputy DSL/Behaviour Lead or, in their absence a member of SLT. The Deputy DSL will then decide with the class teacher who the best person to speak to the child would be.
- Ask their parent to contact the class teacher (in the first instance) to give them the confidence to relay the necessary information. This can be done by the parent writing a note to the teacher in the Homework Diary or emailing the school office to ask the class teacher to contact them.

11.2. Expected staff action

Staff should follow this guidance, which is the same as in the school's anti-bullying policy.

Staff should consider the seriousness of the case and make a quick decision whether to inform the Designated Safeguarding Lead or Deputy DSL/Behavioural Lead immediately before taking any further in-school actions.

All staff should follow the school's Behaviour Policy, which states that each incident should be dealt with by the member of staff who sees the incident or the incident is reported to. If this is done, we hope to potentially stop any form of bullying that may occur.

It is important to deal with a potential situation of bullying immediately and sensitively. It is necessary to gather the information and timeline as soon as possible to get the true facts. It is equally important to deal with it sensitively and think about the language used and the impact of that language on both the children

and the parents when they become involved. Avoid language that may create a 'blame' culture and leave a child labelled.

Staff will talk to the children in a calm and consistent manner. Staff will not be prejudiced, judgmental, dismissive or irresponsible in dealing with such sensitive matters.

11.3. Staff Taking Action

It is important to be prepared for every situation and the potential time it may take.

- Staff will record the incident using the identified paperwork as well as gather witness statements, which will also be recorded on the appropriate paperwork. As much as possible – taking children's age and academic ability into consideration – children should write their accounts in their own hand. The member of staff should then go through it with the child and annotate where needed to ensure that it is indeed a true account.
- Staff will speak to all the children involved, gain a statement from them and use consistent language and open questions for each account.
- Staff will use open questions, 'where, when, why, who'. (What happened? Who observed the incident? What was seen? What was heard? Did anyone intervene?). Do not interrogate or ask leading questions.
- If a member of staff feels they need support in dealing with a situation of this nature, they should ask SLT for support. The expectation is that SLT will be present and offer guidance but that the staff member should still lead the conversation.
- Staff will have a discussion with the child about their actions and use the following restorative questions to allow the child to critically reflect on their actions.
- Staff will record all incidents of a bullying nature on CPOMS to allow the DSL to see all records and gather a complete picture of any/all incidents and patterns.

11.4. The Designated Safeguarding Lead/Deputy Designated Safeguarding Lead (Behaviour Lead)/Member of SLT will:

- Consider the Intent: The DSL/Deputy DSL/Behaviour Lead will review the facts and decide if this has been a deliberate or contrived situation for a young person to be able to harm another?
- Consider any danger that the child may be in
- Decide on the next course of action: if they believe any child to be at risk of significant harm they will follow the school's Safeguarding and Child Protection Policy. If MASH and the police intend to pursue this further, they may ask to interview the children in school or they may ask for parents to come to school to be spoken to
- Make a decision on informing the parents. If the incident is clearly a one-off, then the class teacher may be asked to speak to the parents about the incident in term of what happened and the severity of the incident and any punishment given (in line with the school's behavior policy) If this is a repeated pattern of behavior, the DSL/Deputy DSL will Inform the parents either by telephone call or face-to-face
- The Deputy DSL/Behaviour Lead will keep a record of all identity-based incidents/bullying or sexually-based incidents/bullying

12. Sexting

The term 'sexting' relates to the sending of indecent images, videos and/or written messages with sexually explicit content; these are created and sent electronically. They are often 'shared' via social networking sites and instant messaging services. This must always be referred immediately to the Designated Safeguarding Lead

DSL will follow the UKCCIS: Sexting in schools and colleges 2016 guidance.

Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK (www.gov.uk)

If anyone has a concern that a child may be involved in sexting they should have a conversation with the DSL/Deputy DSL/Behaviour Lead about the next steps. Each situation will be dealt with on an individual basis and judgements will be taken as such. It is very likely that parents will be informed and asked to work together to ensure that the situation is dealt with effectively and efficiently. The child/children involved will be spoken about the effects of their behavior, our Online-Safety learning and the dangers they could be placing themselves in.

13. Where to go for further information

13.1. DfE: Statutory guidance: Working together to safeguard children 2018

https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

13.2. DfE: Statutory guidance: Keeping children safe in education 2022

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1080047/KCSIE_2022_revised.pdf

13.3. DfE: Preventing and Tackling Bullying 2017

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

13.4. DFE Advice for parents regarding cyberbullying

Advice for parents and carers on cyberbullying (publishing.service.gov.uk)

13.5 Anti-Bullying Alliance

https://anti-bullyingalliance.org.uk/