Online Safety Policy

Contents

Date of Last Review: June 2023
Date of Next Review: June 2024

1 Rationale

The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.
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
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.
- Access to content that may be commercial, biased, untrue, unhelpful, or contrary to home or school values

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (e.g. Behaviour, Anti-bullying and Child Protection Policies and Acceptable Use agreements).
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.

2 Development and Monitoring

This online safety policy has been developed by the Computing Subject Lead and the Designated Safeguarding Lead in conjunction with the School Leadership team. As part of this policy, records will be maintained of Online Safety related incidents involving staff and pupils and any incidents recorded will be treated in accordance with our safeguarding procedures. This policy will be reviewed at least annually.
The school will monitor the impact of the policy using:

- Periodic feedback from staff, pupils, parents / carers, governors
- Log of incidents of concern

Role	**Named Person**
Computing Subject Lead	Ben Williams
Designated Safeguarding Lead	Helen Fielder
Head of School	Helen Fielder

3 Scope of the Policy

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

We seek to actively promote and celebrate effective and safe use of the Internet and school systems in line with our school vision and values. Alongside this, we seek to deal with misuse robustly.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils 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 cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The 2011 Education Act increased these powers with regard to the search for and of electronic devices and the deletion of data. In the case of both these acts, action can only be taken in relation to our published Code of Conduct policy, CP and Safeguarding Policy, Acceptable Use Policy, Dignity at work Policy and EH Behaviour Policy.

The school will deal with such incidents within these policies and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

4 Roles and Responsibilities

4.1 Governors

- Governors are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness.

4.2 Head of School / Senior Leaders

- The Head of School is responsible for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Computing Subject Lead/Designated Safeguarding Lead.
- The Head of School is responsible for the implementation and effectiveness of this policy and is also responsible for reporting to the Governing Body on the effectiveness of the policy and, if necessary, make any necessary recommendations re further improvement.
- The Head of School / Senior Leaders are responsible for ensuring that the Computing Subject Lead/ Designated Safeguarding Lead and other relevant staff receive suitable CPD to enable them to carry out their online safety roles.
- The Head of School / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head of School and another member of the Senior Leadership Team must be aware of the procedures to be followed in the event of a serious online safety allegation being made against member of staff. (See Managing Allegations against a member of staff flowcharts guidance - Disciplinary Policy and Procedure)

4.3 Computing Subject Lead + Designated Safeguarding Lead

- Take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Reports to the School Leadership Team serious breaches of the Online Safety Policies
- Provides training and advice for staff
- Liaises with the Local Authority
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Are trained in and share with staff an awareness and understanding of online safety issues and the potential for serious child protection issues that can 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
    - Sexting
    - Revenge pornography
    - Radicalisation (extreme views)
    - CSE

4.4 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring the following:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the Online Safety policy, school ICT and Internet Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the Computing Subject Lead/Designated Safeguarding Lead for investigation / action / sanction
- Digital communications with pupils and parents / carers (email / voice) must be on a professional level
- Children's use of the Internet must always be directly supervised. Moreover, children must be guided to specific, approved online materials and taught how to use safe search engines and techniques to keep them safe and to teach efficient learning methods.
- Ensure that pupils understand and follow, as appropriate for age and ability, the school online safety and acceptable use policy
- Ensure that pupils understand and follow Online Safety rules and they know that if these are not adhered to, sanctions will be implemented in line with our behaviour and anti-bullying policies.
- In lessons, where Internet use is planned, pupils must be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Pupils will be taught skills and techniques for navigating the Internet effectively and safely.

4.5 Pupils

- Are responsible for using the school ICT systems in accordance with the school ICT and Internet Acceptable Use Policy, which they will be expected to agree to before being given access to school systems, where appropriate for age and ability.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so, where appropriate for age and ability.
- Will be supported to follow school rules relating to this policy e.g. safe use of cameras, cyber-bullying etc.
- They with the support of parents/carers must understand that the school's Online Safety Policy covers their actions out of school if related to their membership of the school, where appropriate for age and ability.
- Pupils may not bring mobile devices into school, including e-readers, mobile phones, iPads, iPods, digital cameras or any device enabled to access the Internet, phone network or record media. Smart watches must be disabled to be used as a watch only while in school.

4.6 Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parent briefings, letters, website / local online safety campaigns / literature. Parents and carers will be responsible for:

- being aware of and following the school ICT and Internet Acceptable Use Policy.
- Accessing the school website / on-line pupil records in accordance with the relevant Acceptable Use Policy.

Parents / carers must understand that school has a duty of care to all pupils. The misuse of non-school provided systems, out of hours, will be investigated by the school in line with our behaviour, anti-bullying and safeguarding policies.

5 Education and Training

5.1 Staff

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

- A planned programme of formal online safety training will be made available to staff including safe Internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
- An audit of the online safety training needs of all staff will be carried out regularly
- All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).
- All new staff must receive online safety training as part of their induction programme, ensuring that they fully understand and agree to adhere to the school Online Safety Policy and Acceptable Use Policies
- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.
- Governors will receive training on safe Internet use and online safeguarding issues as part of their safeguarding training.
- The Computing Subject Lead/Safeguarding Lead (or other nominated person) will provide advice/ guidance / training to individuals as required
- Volunteers will receive appropriate training and updates, if applicable.
- More information about safeguarding training is set out in our child protection and safeguarding policy.

5.2 Pupils

Online Safety education will be provided in the following ways, as appropriate to pupils' age and ability:

- A planned online safety programme must be provided as part of Computing/ PHSE / other lessons and must be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Pupils must be taught and encouraged to adopt skills and practices including:
    - Using technology safely, respectfully and responsibly, keeping own and others' personal information private and understanding ways to protect their own and others' online identity, privacy and reputation
    - Using technology positively in line with school, personal and home values
    - Recognising acceptable and unacceptable behaviour
    - Identifying a range of ways to report concerns about content and contact when they have concerns about content or contact on the Internet or other online technologies
    - *Being critically aware of the materials they read and how to validate information before accepting its accuracy.* Information received via the Internet, email or text message requires good information-handling and digital literacy skills. In particular, it may be difficult to determine origin, accuracy and bias as the contextual clues may be missing or difficult to read.
    - Where learning how to access information is not the focus of the learning, teachers will carefully evaluate the usefulness and advantage of using online content - information must be relevant, accessible to all learners, time efficient and lead to deeper learning, e.g. analysis, critical thinking skills.
    - Pupils will use age-appropriate tools to research Internet content and taught how to find such content.
    - The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.
    - The use of Internet derived materials by staff and by pupils will comply with copyright law.
    - Pupils will be taught to acknowledge the source of information used and to respect individuals and intellectual property when using Internet material in their own work.
    - The safe and responsible use of mobile devices and social media and the Internet will also be covered in other subjects where relevant, particularly PSHE.
    - Pupils must be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
    - Pupils must be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
    - Pupils are taught the importance of keeping information such as their password safe and secure.
- Key online safety messages must be reinforced as part of the wider curriculum and school life, including assemblies.
- Rules for the use of ICT systems / internet will be made available for pupils to read
- Staff must act as good role models in their use of ICT and the Internet, demonstrating a high level of respect, responsibility and the school values.
- Where students/ pupils are allowed to freely search the internet, e.g. using search engines, staff must be vigilant in monitoring the content of the websites pupils visit and active in teaching pupils how to do this efficiently and safely.
- It is accepted that from time to time, for good educational reasons, and where appropriate, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (and other relevant person) can temporarily remove those sites from the

filtered list for the period of study. Any request to do so, must be auditable, with clear reasons for the need.

5.3 Parents / Carers

Parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, website, parent briefings
- Reference to external Online Safety websites
- High profile events such as Internet safety day
- Family learning opportunities

If parents have any queries or concerns in relation to online safety, these must be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

6 Technical – Infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- School ICT systems will be managed through the managed service provider, in ways that ensure that the school meets the online safety technical requirements for Wiltshire Local Authority
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems
- Staff will be made responsible 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
- The school maintains and supports the managed filtering service provided by School Care. Any incidents or activities regarding filtering will be handled in accordance with School Care.
- Appropriate security measures are in place, provided by the managed service provider, to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- Guest access to the school network will be authorised by the Network Manager through the provision of limited access guest accounts which do not give access to personal information about pupils or staff.
- The school infrastructure and individual workstations are protected by up-to-date anti- virus software
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy

7 Use of digital photographs and video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the storing, sharing, distribution and publication of those images. Those images must only be taken on school equipment. The personal equipment of staff must not be used for such purposes.
- Care must be taken when taking digital / video images that pupils are appropriately dressed

and are not participating in activities that might bring the individuals or the school into disrepute.

- Pupils and staff must not take, use, share, publish or distribute images of others without their permission. Wherever possible, staff will verbally check if a child is happy for their photo to go on display in school - even though they have parental permission – as this models good practice, dignity and being considerate. If anyone becomes unhappy about their image being shared, it must be removed.
- As part of the admission process and paperwork, written permission from parents or carers will be obtained for the following:
    - photographs of pupils together with their name on school displays and, in their child's, own and other children's learning books and work;
    - photographs of pupils in leaflets, posters, documents, training materials or used by the press
    - photographs of students/pupils on the school website or social media.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs. No image of an individual pupil with be identified by name.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

8 Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. More detailed guidance on the collection, handling and storage of personal data can be found in the school Personal Data Policy.

9 Communications

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Pupils must therefore not use other email systems when in school, or on school systems.
- Users need to be aware that email communications may be monitored.
- Users must immediately report to a DSL or DDSL – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and students or parents / carers must be professional in tone and content and be via official used systems.
- Pupils have their own email addresses as part of the Google Education Suite – however they are limited to communicating within the school domain – this gives a real experience of communicating and collaborating online without contact with anyone outside of school.
- Pupils must be taught about email safety issues, such as the risks attached to the use of personal details. They must also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information must not be placed on the school website on public facing calendars and only official school emails must be identified within it.
- The school allows staff to bring in their own personal devices, including mobile phones, for their own use. These must only be used where no pupils are present.
- Staff must not use their personal devices including mobile phones, to contact a parent/carer unless in an emergency i.e. off-site visit.

10 Cyberbullying

10.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

10.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

10.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

11 Responding to incidents of misuse

There may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse by pupils, staff or any other user appears to involve illegal activity i.e.

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The incident must be dealt with in accordance with the safeguarding policy and if necessary, the police must also be informed.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner.

12 Monitoring and review

This policy will be reviewed annually, or earlier, if necessary, in line with national and/or local updates.

13 Links to other policies

This online safety policy is linked to our:

- School values and ethos
- Child protection and safeguarding policy
- Behaviour policy
- Bullying policy
- PSHE policy
- Child protection policy
- Staff code of conduct for Safer Working Practice
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure