

E-Safety Policy and Procedure

**Statement of intent**

Protecting young people and adults properly means thinking beyond the school environment. Broadband, Wi-Fi and 3/4G connections now mean the world wide web is available anywhere, anytime. Moreover, access to the internet on games consoles, tablets and mobile phones mean it is becoming increasingly difficult to safeguard our pupils from the dangers hidden in cyberspace. To that end, our pupils are not allowed access to unregistered, personal internet enabled devices.

Our pupils will not only be working online in school or at home; their personal devices are not always covered by network protection and it is, therefore, imperative that they are educated on the risks involved with using the internet in their own time and are provided with guidance and a range of strategies on how to act if they see, hear or read something that makes them feel uncomfortable.

E-safety is a child protection issue, and indeed it should not be managed primarily by the ICT team. It should be an extension of general safeguarding and led by the same people, so that, for instance, cyber bullying is considered alongside real-world bullying.

This e-safety Policy seeks to ensure that:

* Pupils are allowed to develop their own protection strategies for when adult supervision and technological protection are not available.
* Information is given on where to seek help and how to report incidents.
* All members of staff, consultants, volunteers and pupils are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
* Guidelines are provided for parents and others on safe practice.
* Technological solutions are regularly reviewed and updated to ensure maintenance of an effective e-safety programme.

Above all, e-safety education should be a continuing feature of both staff development and young people's educational lifelong learning.

The policy:

* Sets out the key principles expected of all members of staff, consultants, volunteers and pupils with respect to the use of ICT-based technologies.
* Safeguards and protects the pupils and staff of the school.
* Assists school staff working with pupils to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
* Sets clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
* Has clear structures to deal with online abuse, such as cyber bullying, which are cross referenced with other school policies.
* Minimises the risk of misplaced or malicious allegations made against adults who work with pupils.

This policy operates in conjunction with other school policies including:

* Acceptable Use of ICT;
* Anti-Bullying Policy & Procedure;
* Complaints and Representation Policy;
* Health and Safety Policy;
* Policy to Counter Radicalisation and Extremism;
* Safeguarding and Child Protection Policy, Procedure and Guidance;
* Whistleblowing Policy.

1. **Teaching and learning**

**Why the internet and digital communications are important**

* 1. The internet is an essential element in education, business and social interaction. The school has a duty to provide pupils with quality internet access as part of their learning experience.
  2. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
  3. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
  4. Staff model safe and responsible behaviour in their use of technology during lessons.
  5. Parents/Carers and pupils will sign an Internet Access / Computer Network Pupils’ Rules for Use consent form prior to admission.

**Internet use will enhance learning**

* 1. The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
  2. Pupils will be aware of expected and unexpected behaviour when using the internet and given clear objectives for internet use.
  3. Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
  4. Pupils will be shown how to publish and present information to a wider audience.

**Pupils will be taught how to evaluate internet content**

* 1. The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
  2. Pupils will be taught the importance of cross-checking information before accepting its accuracy.
  3. Pupils will be taught how to report unpleasant internet content to an appropriate adult. This can be done anonymously, or in person, and will be treated in confidence.

1. **Managing internet access**

**Information system security**

* 1. School ICT systems security will be reviewed regularly.
  2. Virus protection will be updated regularly.

**Email**

* 1. Pupils may not use e-mail in the school.
  2. The school:
* Provides staff with an email account for their professional use and makes clear personal email should be through a separate account.
* Will contact the Police if one of our staff receives an email that it considers is particularly disturbing or breaks the law.
* Will ensure that email accounts are maintained and up-to-date.
* Reports messages relating to or in support of illegal activities to the relevant authority and if necessary to the Police.
* Knows that spam, phishing and virus attachments can make emails dangerous.
* Will treat incoming emails as suspicious and attachments not opened unless the author is known.

**Published content on the school website and social media platform**

* 1. Staff or pupil personal contact information will not be published. The contact details given online should be the school office.
  2. The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate, and the quality of presentation is maintained.
  3. Uploading of information is restricted.
  4. The school website complies with the The Education (Independent School Standards) Regulations
  5. Most material is the school’s own work; where others’ work is published or linked to, we credit the sources used and state clearly the author's identity or status.
  6. The point of contact on the website is the school address and telephone number. The school uses a general email contact address; [admin@melchetcourt.com](mailto:admin@melchetcourt.com) / [enquiries@melchetcourt.com](mailto:enquiries@melchetcourt.com).
  7. Photographs published on the web do not have full names attached.

**Publishing pupils’ images and work**

* 1. Photographs that include pupils will be selected carefully so as to maintain pupil dignity and prevent their image being misused. The school will consider using group photographs rather than full-face photos of individual children.
  2. Pupils’ full names will not be used anywhere online, particularly in association with photographs or footage. E.g. school newsletter, school YouTube channel.
  3. Written permission from parents/carers will be obtained prior to admission before photographs, footage or work of pupils are published on the school website or social media.
  4. The school does not use pupils’ names when saving images in the file names or in the tags when publishing online.
  5. Parents/carers should be clearly informed of the school policy on image taking and publishing.
  6. Members of staff are forbidden from taking or storing images or footage of pupils or pupil work on their personal devices.
  7. Staff sign to confirm they have read and understood school policy in relation to the use of ICT; primarily Digital Communication Policy and Staff Behaviour Policy.
  8. If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high-profile publications, it is the responsibility of the parents/carers or pupil to withdraw consent at the point of which their placement ends.
  9. The school blocks/filters access to social networking sites or newsgroups unless there is a specific approved educational purpose.

**Social networking and personal publishing**

* 1. The school will control access to social networking sites and consider how to educate pupils in their safe use.
  2. Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for pupils.
  3. Pupils will be advised to use nicknames and avatars when using social networking sites.
  4. The school prohibits staff from accepting and initiating invitations to “friend” current pupils, or current pupils’ family members / friends.
  5. Staff are instructed not to run social network spaces for pupil use on a personal basis or to open their own spaces to their pupils, but to use the school’s preferred system for such communications.

**Managing filtering**

* 1. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing emerging technologies**

* 1. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
  2. The SMT should note that technologies, such as mobile phones with wireless internet access, can bypass school filtering systems and present a new route to undesirable material and communications.
  3. Mobile phones and any multimedia devices will not be used during school time.

**Protecting personal data**

* 1. Personal data will be recorded, processed, transferred and made available according to the GDPR and the Data Protection Act 2018.

# **Personal devices and mobile phones**

* 1. The school reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or cyber bullying.

1. **Policy decisions**

**Authorising internet access**

* 1. All staff will read and agree an understanding of policy and procedures before using any school ICT resource. This will be conducted by the Systems Administrator as part of the employee’s induction process.
  2. The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
  3. Access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

**Assessing risks**

* 1. The school will take all reasonable precautions to prevent access to inappropriate material; however, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of internet access.
  2. The school should audit ICT use to establish if the e-safety Policy is adequate and that the implementation of the e-safety Policy is appropriate and effective.

**Handling e-safety complaints**

* 1. Complaints of internet misuse will be dealt with by a Senior Manager.
  2. A complaint about staff misuse must be referred to the Head of Pastoral Care in the first instance. In the event that the complaint pertains to the Head of Pastoral Care, the Headteacher must be duly informed. Similarly, the Chairman of the Board should be in receipt of the complaint if the Headteacher is the subject of the complaint.
  3. Complaints of a child protection nature must be dealt with in accordance with the school’s safeguarding and child protection procedures and the Designated Safeguarding Lead informed.
  4. Pupils and parents will be informed of the consequences for pupils misusing the internet.

1. **Pupil online safety curriculum**

**Teaching and learning**

* 1. The school has a clear, progressive online safety education programme as part of the computing/PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
* To STOP and THINK before they CLICK.
* To develop a range of strategies to evaluate and verify information before accepting its accuracy.
* To be aware that the author of a website/page may have a bias or purpose and to develop skills to recognise what that may be.
* To know how to narrow down or refine a search.
* To understand how search engines work and to understand that this affects the results they see at the top of the listings.
* To understand expected behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour.
* To understand how photographs can be manipulated and how web content can attract the wrong sort of attention.
* To understand why online ‘friends’ may not be who they say they are and to understand why they should be careful in online environments.
* To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos, and to know how to ensure they have turned-on privacy settings.
* To understand why they must not post pictures or videos of others without their permission.
* To know not to download any files – such as music files – without permission.
* To have strategies for dealing with receipt of inappropriate materials and the importance of not sharing and the legal implications should they do so.
* To understand why and how some people will ‘groom’ young people for exploitation.
* To understand the impact of cyber bullying, sexting, extremism and trolling and know how to seek help if they are affected by any form of cyber bullying.
* To develop their digital resilience to recognise and manage the risks they come across when they socialise, explore or work online.
* To know how to report any abuse, including cyber bullying, and how to seek help if they experience problems when using the internet and related technologies, i.e. parent/carer, teacher or trusted staff member, or an organisation such as Childline or the CLICK CEOP button.
  1. Teachers plan internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
  2. All staff will model safe and responsible behaviour in their own use of technology during lessons.

**Online risks**

* 1. The school recognises that pupils increasingly use a range of technology such as mobile phones, tablets, games consoles and computers. It will teach appropriate use of these technologies for entertainment and education but will also raise awareness of associated risk primarily in PSHE and ICT.

# **Cyber bullying and abuse**

* 1. Cyber bullying can be defined as “Any form of bullying which takes place online or through smartphones and tablets.” - BullyingUK
  2. Complaints of cyber bullying are dealt with in accordance with the school’s Anti-Bullying Policy and Procedure. Complaints of a child protection nature must be dealt with in accordance with the school’s safeguarding and child protection procedures and the Designated Safeguarding Lead informed.
  3. Through the curriculum, pupils are taught to tell a responsible adult if they receive inappropriate, abusive or harmful emails or text messages.
  4. Posters providing information about how to get help from Childline, ThinkUKnow and the NSPCC are displayed in corridors, communal areas and residential areas.
  5. All incidents of cyber bullying reported to the school will be recorded.

**Online grooming and sexting**

* 1. Sexting between pupils will be managed through the school’s Safeguarding and Child Protection Policy, Procedure and Guidance.
  2. All staff are made aware of the manner in which pupils can be groomed online and all concerns are to be reported immediately to the DSL.
  3. There are clear procedures in place to support pupils and staff affected by exploitation and sexting.
  4. All incidents of sexting reported to the school will be recorded.

1. **Communications policy**

**Introducing the e-safety policy to pupils**

* 1. E-safety rules and guidance posters will be displayed in corridors, communal areas and residential areas and discussed with pupils regularly.
  2. Pupils will be informed that network and internet use will be monitored and appropriately followed up.
  3. An awareness of e-safety is a cross-curricular event each year when the school observes National Safer Internet Day.
  4. E-safety training will be embedded within the computing and PSHE schemes of work in line with national curriculum expectations.

# **Staff and the e-safety policy**

* 1. All staff will be given the school’s e-safety Policy and have its importance explained.
  2. Staff must be informed that network and internet traffic can be monitored and traced to the individual user.
  3. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
  4. Staff will always use a child friendly safe search engine when accessing the web with pupils.

# **Enlisting parents’ support**

* 1. The school will maintain a list on the school’s website of e-safety resources for parents/carers.
  2. The school will ask all new parents/carers to sign the parent/pupil agreement when they register their child with the school.

This review: JF/KT/AH January 2020

Approved by Governors: January 2020

**Useful Resources for Teachers and Parents**

|  |  |
| --- | --- |
| **Resource** | **Website** |
| Child Exploitation and Online Protection Centre | [www.ceop.gov.uk/](http://www.ceop.gov.uk/) |
| Childnet | [www.childnet-int.org/](http://www.childnet-int.org/) |
| Digizen | [www.digizen.org/](http://www.digizen.org/) |
| Kidsmart | [www.kidsmart.org.uk/](http://www.kidsmart.org.uk/) |
| Think U Know | [www.thinkuknow.co.uk/](http://www.thinkuknow.co.uk/) |
| Family Online Safety Institute | <http://www.fosi.org> |
| Internet Watch Foundation | [www.iwf.org.uk](http://www.iwf.org.uk) |
| Internet Safety Zone | [www.internetsafetyzone.com](http://www.internetsafetyzone.com) |
| Vodafone digital parenting | [www.vodafone.com/content/digital-parenting.html](https://www.vodafone.com/content/digital-parenting.html) |
| NSPCC - Share Aware | [www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware](https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware) |
| Parent Zone | [www.theparentzone.co.uk/school](http://www.theparentzone.co.uk/school) |