

# **Acceptable Use Policy**

---

UPDATED: March 2011

## 1 Table of Contents

---

1	What is an AUP (Acceptable Use Policy)? .....	3
2	Why have an AUP? .....	3
3	Aims of this policy.....	4
4	Roles and responsibilities of the school.....	4
4.1	Vorstand and Head .....	4
4.2	Head of ICT .....	5
4.3	Staff or adults .....	5
4.4	School pupils.....	7
5	Appropriate use by staff or adults .....	7
5.1	In the event of inappropriate use .....	7
6	Appropriate use by pupils .....	8
6.1	In the event of inappropriate use .....	8
7	The curriculum and tools for learning.....	9
7.1	Internet use .....	9
7.2	E-mail use .....	9
7.3	Mobile phones and other technologies.....	10
7.4	Video and photographs.....	10
8	Filtering and safeguarding measures .....	10
9	Monitoring.....	11
10	School library .....	11
11	Parents.....	11
11.1	Roles .....	11
11.2	Support.....	11
12	Links to other policies.....	12
12.1	Behaviour and Anti-Bullying Policies .....	12
12.2	Allegation Procedures and the Child Protection Policy .....	12
12.3	School website.....	12
12.4	External websites .....	12
12.5	Disciplinary Procedure for All School Based Staff .....	<b>Error! Bookmark not defined.</b>

## **2 What is an AUP (Acceptable Use Policy)?**

---

This Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the internet, e-mail, instant messaging and other social networking spaces, mobile phones and games) to safeguard adults and children at Berlin British School. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies. It also explains procedures for any unacceptable or misuse of these technologies by adults or children.

## **3 Why have an AUP?**

---

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or mobile devices.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

It is also important that adults are clear about the procedures, for example only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst Berlin British School acknowledges that it will endeavor to safeguard against all risks it will never be able to completely eliminate them. Any incidents that may come to its notice will be dealt with quickly and according to policy to ensure we continue to protect children.

It is the duty of the school to ensure that pupils are protected from potential harm whilst they are on school premises. Therefore, the involvement of children and parent/carers is also vital to the successful use of on-line technologies. This policy thus also aims to inform how parents/carers and children are part of the procedures and how children are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect children and adults from potential and known risks.

## 4 Aims of this policy

---

- To ensure the safeguarding of all children within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.

To develop links with parents/carers and the wider community to ensure input into policies and procedures, with continued awareness of on-line technologies.

## 5 Roles and responsibilities of the school

---

### 5.1 Vorstand and Head

It is the overall responsibility of the Head with the Vorstand to ensure that there is an overview of e-safety (as part of the wider remit of Child Protection) across the school, with further responsibilities as follows:

- 5.1.1 **It is the delegated responsibility of the Head of ICT to implement agreed policies, procedures, staff training and curriculum requirements, and to take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment. Time and resources are provided to the Head of ICT to ensure that this is done.**
- 5.1.2 **The Head, along with the Vorstand, has determined that there should be a standard disclaimer on all e-mails stating that the views expressed are not necessarily those of the school.**
- 5.1.3 **The Head is responsible for promoting e-safety across the curriculum and has an awareness of how this is being developed, linked with the school Development Plan.**
- 5.1.4 **The Head will inform the Vorstand at their meetings about the progress of, or any updates to, the e-safety curriculum (via PSHE or ICT) and ensure Vorstand members know how this relates to child protection. Vorstand members will be made aware of e-safety developments.**
- 5.1.5 **The Vorstand must ensure Child Protection includes a thorough awareness of e-safety and how it is being addressed within the school, as it is the responsibility of the Vorstand to ensure that all Child Protection guidance and practices are applied.**
- 5.1.6 **An e-safety Vorstand member will ensure the school has an AUP with appropriate strategies which define the roles, responsibilities for the management, and implementation and safety for using ICT, including:**
  - Firewalls
  - Anti-virus, anti-spyware and email monitoring software
  - Web proxies to filter web access
  - Using an accredited ISP (Internet Service Provider)
  - Awareness of wireless technology issues

- A clear policy on using personal devices
- Assurance that any misuse or incident has been dealt with appropriately, according to school policy and procedures, and appropriate action is taken even to the extent of suspending a member of staff, informing the police or involving parents/carers.

## **5.2 Head of ICT**

**It is the role of the Head of ICT to:**

- 5.2.1 Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-safety, for parents to feel informed and know where to go for advice.**
- 5.2.2 Ensure that filtering is set to the correct level for staff and pupils in the initial set up of a network, stand-alone PC, staff/children laptops or ensure the technician is informed and carries out work as directed.**
- 5.2.3 Ensure that all adults are aware of the filtering levels and why they are there to protect pupils.**
- 5.2.4 Report issues and update the Head on a regular basis.**
- 5.2.5 Liaise with the Heads of School so that policies and procedures are up-to-date to take account of any emerging issues and technologies.**
- 5.2.6 Update staff training according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.**
- 5.2.7 Ensure transparent monitoring of the internet and on-line technologies.**
- 5.2.8 Keep a log of incidents for analysis to help inform future development and safeguarding, where risks can be identified.**
- 5.2.9 Ensure there is appropriate and up-to-date anti-virus, anti-spyware and monitoring software on the network, stand-alone PCs and teacher/child laptops, and that this is reviewed and updated on a regular basis.**
- 5.2.10 Ensure that staff can check for viruses on laptops, stand-alone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.**

## **5.3 Staff or adults**

**It is the responsibility of all adults within the school to:**

- 5.3.1 Ensure that they know who the Designated Person for Child Protection is within school and on the Vorstand so that any misuse or incidents which involve a pupil can be reported. Where an allegation is made against a member of staff it should be reported immediately to the Head. In the event of an allegation made against the Head, the Chair of the Vorstand must be informed immediately.
- 5.3.2 Be familiar with the behaviour, anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed. In the event that a procedure is unknown, they will refer to the Head immediately, who should then follow the Allegations Procedure (12.5).
- 5.3.3 Check the filtering levels are appropriate for their pupils and are set at the correct level, and to report any concerns to the Head of ICT.
- 5.3.4 Alert the Head of ICT of any new or arising issues and risks that may need to be included within policies and procedures.
- 5.3.5 Ensure that pupils are protected and supported in their use of on-line technologies, and that they know how to use them in a safe and responsible manner.
- 5.3.6 Be up-to-date with e-safety knowledge that is appropriate for the age group.
- 5.3.7 Help to ensure that the use of blanket emails is kept to a minimum and that an appropriate tone is used when communicating by email.
- 5.3.8 Sign an Acceptable Use Statement to show that they agree with and accept the rules for staff using non-personal equipment, within the school environment.
- 5.3.9 Use electronic communications in an appropriate way.
- 5.3.10 Protect confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- 5.3.11 Report accidental access to inappropriate materials to the Head of ICT and ICT Support in order that inappropriate sites are added to the restricted list.
- 5.3.12 Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the internet on a regular basis, especially when not connected to the school network.
- 5.3.13 Report incidents of personally directed "bullying" or other inappropriate behaviour via the Internet or other technologies.
- 5.3.14 Monitor the information pupils upload onto web sites and is e-mailed to other people, and help to ensure that it does not include any personal information including:
- full name (first name is acceptable, without a photograph)
  - address
  - telephone number
  - e-mail address
  - school
  - clubs attended and where

- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

**5.3.15 Help to monitor the uploading of photographs on to the internet.**

**5.3.16 Help to ensure that first names only are posted on the school website.**

## **5.4 School pupils**

**Pupils are:**

**5.4.1 Involved in the review of our Acceptable Use Rules through the School Council, in line with this policy being reviewed and updated.**

**5.4.2 Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school for the first time.**

**5.4.3 Taught to use the internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.**

**5.4.4 Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away.**

## **6 Appropriate use by staff or adults**

---

Staff members have access to the network so that they can access age appropriate resources for their classes. They have a password to access a filtered Internet service and know that this should not be disclosed to anyone. They should not leave a computer or other device unattended whilst they are logged in.

All staff receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed and returned to school, where it is kept on file, with a signed copy returned to the member of staff. The Acceptable Use Rules are displayed in the staff room as a reminder that staff members need to safeguard against potential allegations.

### **6.1 In the event of inappropriate use**

If a member of staff is believed to have misused the internet or network in an abusive or illegal manner from school, a report must be made to the Head, Head of School and Head of ICT immediately. Then the Allegations Procedure and the Child Protection Policy must be followed to deal with any misconduct, and all appropriate authorities contacted.

In the event of minor infringement or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

## **7 Appropriate use by pupils**

---

Acceptable Use Rules and the letter for children and parents/carers are outlined in the Appendices and detail how pupils are expected to use the Internet and other technologies within school, which includes downloading or printing of any materials. The rules are there for pupils to understand what is expected of their behaviour and attitude when using the internet which then enables them to take responsibility for their own actions; for example, knowing what is polite to write in an e-mail to another pupil or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences of doing so.

The rules will be on display within the classrooms and in the computer suite.

We want our parents/carers to support our rules with their child or young person, as reflected in both parents/carers and pupils signing the Acceptable Use Rules, so that it is clear that the rules are accepted by the pupil and the parent/carer.

We hope that parents/carers will suggest amendments or updates to the rules so that they feel the rules are appropriate to the technologies being used and reflect any potential issues that parents/carers feel should be addressed.

The downloading of materials, for example, music files and photographs, needs to be appropriate and 'fit for purpose', based on research for school work, and be copyright free. File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free, in or beyond school.

The School Council is actively encouraged to be involved in discussing the acceptable use of on-line technologies and the sanctions for misusing them.

### **7.1 In the event of inappropriate use**

Should a pupil be found to misuse the on-line facilities whilst at school appropriate sanctions will be applied.

If a pupil accidentally accesses inappropriate materials the pupil will report this to an adult immediately and take appropriate action to hide the screen or close the window. Deliberate abuse or damage of school equipment will result in parents/carers being billed for the replacement costs of the equipment.

Pupils are taught and encouraged to consider the implications for misusing the internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

## 8 The curriculum and tools for learning

---

### 8.1 Internet use

We teach our pupils how to use the internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding, and communicating effectively in order to further learning, through ICT and/or PSHE lessons. The following concepts, skills and competencies are taught by the end of Year 6 or Year 11:

- internet literacy
- making good judgments about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues
- file-sharing and downloading illegal content
- uploading information – knowing what is safe to upload and not upload personal information
- where to go for advice and how to report abuse

Key Stage 3 requires pupils to learn e-safety as part of the National Curriculum for ICT.

The [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) resources are used, with free training provided to teachers/adults for the delivery of these lessons. Further training advice can be sought from the Head of ICT or by going to the website.

These skills and competencies are taught within the curriculum so that pupils have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner.

### 8.2 E-mail use

We have school e-mail addresses for pupils as part of their entitlement to understand different ways of communicating and using ICT, and so they may share and present information in different forms.

Pupils must use their school issued e-mail addresses for any communication from or to school only. A breach of this will result in sanctions. Parents/carers are encouraged to be involved with monitoring of e-mails.

Teachers monitor students' use of e-mails. The school operates monitoring software that is used to identify inappropriate terms and the Head of ICT has an overview of users.

### **8.3 Mobile phones and other technologies**

The use of mobile phones is allowed in our school outside the classroom and lesson times. Staff members are not allowed to use their personal numbers to contact children and young people under any circumstances. It is also our policy to ensure that we educate our children and young people to understand the use of a public domain and the consequences of misusing it, including the legal implications and law enforcement.

### **8.4 Video and photographs**

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to digital cameras. It is not appropriate for staff to use their personal mobiles or other personal equipment to take photographs.

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded and stored on the school network should not have a file name of a pupil. Photographs should only ever include the pupil's first name.

Group photographs are preferable to individual children and should not be of any compromising positions or in inappropriate clothing. School will need to decide how photographs will be used, including where they will be stored and when they will be deleted. Images should be stored within the "School Wide Resources" area on the network. Image files must not be stored on local machines.

## **9 Filtering and safeguarding measures**

---

Please refer to the Acceptable Use Rules for Staff and Children for the appropriate use of the network.

The school's internet has a filter system which is set at an age appropriate level so that inappropriate content is filtered, and tools are appropriate to the age of the child.

Anti-virus, anti-spyware, web and email monitoring software is used on the school's network, stand alone PCs, and laptops, and is updated on a regular basis. A firewall ensures information about our children and the school cannot be accessed by unauthorised users.

Encryption codes on wireless systems prevent hacking.

## 10 Monitoring

---

The Head of ICT and/or a senior member of staff monitor the use of on-line technologies by children and young people and staff, on a regular basis.

The use of 'Forensic or Securus' software, for example, has been employed by school. The Head of ICT will monitor the use of the internet on a regular basis, with alerts sent in real-time to highlight any potential misuse or risk.

## 11 School library

---

The computers in the school library are protected in line with the school network.

Where software requiring a pupil login is used, it is password protected so that the pupil is only able to access him/herself as a user. Pupils are taught not to divulge their own passwords.

## 12 Parents

---

### 12.1 Roles

Each pupil has access to a copy of the school's Acceptable Usage Policy rules. This needs to be read with the parent/carer, and then signed and returned to school confirming both an understanding and acceptance of the rules. It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted. School will keep a record of the signed forms.

### 12.2 Support

As part of the approach to developing e-safety awareness with pupils, the school may offer parents the opportunity to find out more about how they can support the school to keep their child safe whilst using on-line technologies beyond school. The school wishes to promote a positive attitude to using the World Wide Web and therefore wants parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly. To that end, the school will hold Parent/Carer Information Evenings. Use of the Childnet International 'KnowITAll for Parents' CD/on-line materials (<http://www.childnet-int.org.uk/kia/parents/cd/>) may also be made to deliver key messages and raise awareness for parents/carers and the community. Part of the evening is to provide parents with information on how the school protects pupils using the learning platform facilities, such as the internet and e-mail. It also is an opportunity to explore how the school is teaching pupils to be safe and responsible Internet users, and how this may be extended to use beyond the school environment.

Parents should be aware that the school cannot take responsibility for a pupil's misuse or abuse of IT equipment when they are not on the school premises. This includes social networking with other pupils.

## **13 Links to other policies**

---

### **13.1 Behaviour and Anti-Bullying Policies**

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. The school does not treat on-line misbehaviour any differently from off-line, and has the same expectations of behaviour.

### **13.2 Allegation Procedures and the Child Protection Policy**

Please refer to the Disciplinary Procedure in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or pupil about a member of staff.

Allegations should be reported to the Head, Head of School and Head of ICT immediately, or Chair of Vorstand in the event of the allegation being made about the Head.

No personal equipment belonging to staff should be used when contacting pupils about homework or any other school issues either in or beyond school. We follow this information to protect our staff members from potential allegations of misconduct by a pupil or parent.

Please refer to the Child Protection Policy for the correct procedure in the event of a breach of child safety, and inform the designated person for child protection within school immediately.

### **13.3 School website**

The uploading of images to the school website is subject to the same rules as uploading to any personal on-line space.

### **13.4 External websites**

In the event that a member of staff finds him or herself or another adult on an external website, such as 'Rate My Teacher', users are encouraged to report incidents to the Head.