Acceptable Use Policy

Reddam House Berkshire is committed to safeguarding and promoting the welfare of children and young people and expects all staff, volunteers, students and visitors to share this commitment.

All outcomes generated by this document must take account of and contribute to safeguarding and promoting the welfare of children and young people at Reddam House Berkshire.

Contents

Scope

This policy applies to all members of the school community, including staff, students, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online Behaviour

As a member of the school community you should follow these principles in all your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, material that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. **Do not share** photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or reach the personal email addresses or social media accounts of staff. Staff should inform the DSL if a student requests to follow them on social media.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your device to the network) you should follow these principles:

- Only access school IT systems using your username and password. Do not share your username or password with anyone else.
- Staff should not share passwords for any other wifi network with students -all students should be on 'student wifi' where filtering and monitoring takes place. Staff should report to the DSL if they have evidence or suspicions that any student is using a different wifi network.

- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not try to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy, Mobile Device and Social Media Policy, Safeguarding Policies and Anti-Bullying Policy.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. Also, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the school's DSL (Mrs Towse). Reports will be treated with confidence.

Complaints relating to all aspects of E-Safety

As with all issues of safety at Reddam House Berkshire, if a member of staff, a student or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Head of School in the first instance, who will liaise with the Principal and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around, e-safety will be recorded using CPOMS (see Safeguarding Policy) and reported to the school's Designated Safeguarding Lead following the school's Safeguarding Policies.

Acceptable Use Agreements

Student Acceptable Use Agreement

The Acceptable Use Agreement is held as a series of answers to questions on a Microsoft Form. This is distributed to all students Year 5 up at the start of each academic year (or upon starting if mid-year).

For my safety:

- I understand that the school will monitor my use of the ICT systems, e-mail and other digital communications.
- I will not tell anyone my username or password, nor will I try to use any other person's username and password.
- I will be aware of 'stranger danger' when I am communicating online.
- I will not give out any personal information (e.g. home address and telephone number) about myself or anyone else when online to people I do not know or in a public forum.
- I will not arrange to meet people in person that I have met and communicated with online.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

Respecting everyone's rights to use technology as a resource:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube) unless I have the permission of a member of staff to do so.

Acting as I expect others to behave toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

Keeping secure and safe when using technology in school:

- I will only use approved e-mail or message accounts on the school system.
- I will only use 'student wifi' and will not attempt to access any other wifi within school.
- I will only use my handheld/external devices (e.g. mobile phones, USB devices, etc.) in school if I have permission and I understand that if I do use my own devices in school, I must follow the rules as if I was using school equipment.
- I will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software.
- I will not open any attachments to e-mails unless given permission to do so by my teacher or parents and I know and trust the person/organisation that sent the e-mail.
- I will ask for permission before sending an e-mail to an external person/organisation

- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer, nor will I try to alter computer settings.
- I will immediately tell a staff member if I receive an offensive or suspicious e-mail or message.

Using the internet for research or recreation:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate.
- I should ensure that I have permission to use the original work of others in my work.
- Where work is protected by copyright, I will not try to download copies (including music and videos) and will respect copyright and intellectual property rights.

Taking responsibility for my actions, both in and out of school:

- I understand that the school also has the right to act against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they include my membership of the school community (e.g. cyberbullying, inappropriate use of images and/or personal information).
- I understand that if I break these rules, I will be subject to disciplinary action as outlined in the school's Behaviour Policy. This may also include loss of access to the school network/internet.

Filtering & monitoring:

- I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems.
- I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
- I understand that my activity on the ICT systems will be monitored and that the school will act if they have concerns about any possible breaches of the Acceptable Use Policy. I will adopt the safe use of the internet and digital technologies at home and will inform the school if I have concerns over my e-safety.

I have read and understood the above and agree to follow the rules outlined.

Name:	
Signature:	
Date:	

Parent/Carer Acceptable Use Agreement

The Acceptable Use Agreement is held as a series of answers to questions on a Microsoft Form. This is distributed to all students Year 5 up at the start of each academic year (or upon starting if mid-year).

The school seeks to ensure that students have good access to ICT to enhance their learning and, in return, expects students to agree to be responsible users. A copy of the Student Acceptable Use Agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

===

Acceptance of Use Form

Parent/Carer's Name	
Student's Name:	

As the parent/carer of the above student, I understand that my son/daughter will have access to the internet and ICT systems at school.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt the safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

'As a parent, I support school safeguarding policies and I will ensure that I monitor my child's use of the internet (including social networking) outside of school. I will act as a positive role model for my child where appropriate'

Signature:	
Date:	

Staff Acceptable Use Agreement

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this code of conduct as a form. Members of staff should consult the school's e-Safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, e-mail, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Principal.
- I understand that my use of school information systems, internet and e-mail may be monitored and recorded to ensure policy compliance.
- I will respect system security, and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware unless authorised, e.g. on a school laptop.
- I will ensure that personal data, particularly that of students, is stored securely through encryption and password and is used appropriately, whether in school, taken off the school premises or accessed remotely following the school e-Safety policy.
- I will respect copyright and intellectual property rights.
- I will ensure that electronic communications with students (including e-mail, instant messaging and social networking) and any comments on the web (including websites, blogs and social networking) are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure that student use of the internet is consistent with the school's e-Safety Policy.
- When working with students, I will carefully monitor and scrutinise what students are accessing on the internet including checking the history of pages when necessary.
- I will ensure that computer monitor screens are readily visible when under supervision, to enable monitoring of what the children are accessing.
- I know what to do if offensive or inappropriate materials are found on screen or printer.
- I will report any incidents of concern regarding students' safety to the appropriate person, e.g. DSL and Head of School and record on CPOMS.
-

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes the unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sounds.

Name:		Date:	
Signature:			