St Crispin's School Policy

Staff ICT Acceptable Use Policy

Version Number	Date Created	Changes or reason for Update	Date Approved
V1.4	07/2010	Issued in School Format for first time	07/2010
V1.5	02/2012	Minor changes to wording	02/2012
V1.6	07/2012	First major update	09/2012
V1.7	09/2014	Clarification text in Sect 5.2. Remove redundant text in 8.1	10/11/14
V2	10/2016	No changes made	7/11/2016

Next Review of this Policy is due 10/2018

1. Purpose

This Acceptable Use Policy is aimed at encouraging responsible behaviour and good practice. It has been created with the view to:

1.1 Ensure compliance and enforcement of relevant legislation which include but is not limited to the Computer Misuse Act and the Data Protection Act;
1.2 Ensure the safety and integrity of students, staff and others;
1.3 Prevent damage to the school and its physical property.

2. Policy Statement

2.1 Staff will be notified via the staff intranet and email of any changes made to this policy.
2.2 This Acceptable Use Policy replaces and supersedes all previous versions.

3. Electronic communication (including e-mail, telephony and social media)

3.1 All members of staff will be provided with email services for school related communication. All messages sent from within school must be sent using the school email system. All school related messages, whether sent within or outside school must be sent using the school email system. No other communication system (hotmail, gmail Facebook, Twitter etc) is to be used. The only exception to this rule is that the Communications Officer will use the official St Crispin's Facebook and Twitter sites to publish school related information.

3.2 All email communication between staff and students (including Sixth Form students) MUST be via the school email system. External (private) email accounts (whether they be staff or student) must never be used. This restriction also applies to ALL social networking sites such as Facebook, Twitter etc. The school VLE may also be used to provide feedback to students on work submitted. Teachers may also use other facilities within the VLE to assess student work and provide feedback. Eg discussion topics in forums.

3.3 Communication between staff and students via personal mobile phones is not allowed under any circumstances. However, teachers may give

students the school mobile number for contact in an emergency when out on trips.

3.4 These regulations apply for all students until the 31st August of the year that the cohort to which they belong reaches Year 13. IMPORTANT: This applies for every student, including those leaving the school prior to this date

3.5 The use of e-mail for personal purposes is permitted but must be reasonable

3.6 The transmission of confidential information via e-mail to unauthorised persons is strictly prohibited.

3.7 While St Crispin's School respects the privacy of staff, where there is reason for concern, the school reserves the right to monitor and intercept e-mail communication. Email use should therefore be appropriate at all times.

3.8 Any e-mail communication made must not bring the School into disrepute; this includes anything libellous, defamatory or criminal.

3.9 During a typical working day, all members of staff must check their email at least twice, preferably in the morning and at the end of the day. Training in the use of email will be provided for any member of staff who requests it.

3.10 Staff must, where possible, acknowledge receipt of emails within 24 hours and, if appropriate, give an indication of when a full response can be expected.

3.11 All members of staff must check the staff intranet for announcements at regular intervals during the week.

3.12 Computer based documents (e.g. minutes and agendas) will be issued by email. These documents will also be stored in an appropriate location on the network/intranet

3.13 Staff members must consider carefully to whom a mail is cc'd. The school does not want to create a situation where people receive excessive amounts of messages in their inboxes. The staff intranet can be used for general announcements.

3.14 The 'All Staff' alias should not be used unless necessary. Mails should only be sent to the groups who need to receive them.

3.15 Email should be used to replace handwritten notes left in pigeonholes.

3.16 Any email sent to students must remain at a professional level.

3.17 It is acceptable to send an email to a parent as an alternative to a telephone call. However, emails must not be used as a replacement for letters that are currently sent to parents. The appropriate HoD or HoY must be cc'd in any email to parents.

3.18 Staff should not distribute large documents as attachments – these should be placed on the school network or the intranet as shared documents.

4. Internet Access

4.1 St Crispin's School will only provide access to the Internet on receipt of a signed Acceptable Use Policy. Failure to sign the AUP after a reasonable period of time will result in suspension of the network account

4.2 All Internet access is logged for the purposes of maintaining standards of security and acceptable use.

4.3 Attempts to access inappropriate websites or websites which attempt to bypass filtering systems constitute a breach of this Acceptable Use Policy.

4.4 Inappropriate websites referred to in **4.3** include, but are not limited to any site which contains:

- Pornographic Material (of either a legal or illegal nature);
- Material which incites hatred or discrimination;
- Material which promotes illegal activity;
- Material which is in breach of the Copyright Designs and Patents Act 1998;
- Material which is degrading to persons or groups of;

4.5 Members of staff are required to report any website that they become aware of, which is not filtered, that is deemed inappropriate as per the criteria stated within **4.4**.

4.6 Staff should refrain from downloading large files during school hours as this may affect the quality of service for other users.

4.7 While St Crispin's School, in conjunction with Wokingham LA, uses sophisticated filtering technology and takes all precautions to ensure that users only access appropriate material, it is not possible to guarantee that unsuitable material will be inaccessible. Neither the School nor Wokingham LA can accept liability for the material accessed, or any consequences of such access.

4.8 The importance of E-Safety must be recognized. Staff must endeavour to promote good E-Safety practice to students at appropriate times. Staff must also ensure that they remain up to date with the guidance

provided by the school on what advice to give to students. Staff are required to immediately report to the school any incidents which may be deemed to be unsafe use of the internet and/or email by the students.

5. Network Access

5.1 Members of staff are issued with a network user name and password which must only be used by the member of staff they are issued to. Liability remains with the logged in user.

5.2 Allowing another person (including other staff and students) to use your login is a severe breach of this Acceptable Use Policy and contravenes legislation. This includes 'loaning' a login to a student (e.g. giving a student a laptop which has been logged in with a staff ID is strictly forbidden and may lead to disciplinary action), or to a school visitor. In the latter case, a temporary login can be requested from IT Support using the call logging system (please give 24 hours notice)

5.3 Passwords must never be divulged to anyone at anytime. If it is suspected that a password has been compromised it must be changed immediately.

5.4 Staff will not attempt to download or install software onto the network or IT Equipment. Staff laptops allow the registered keeper to install software locally on that machine only. This software must be legal and a copy of the relevant software license be made available on request

5.5 It is prohibited to copy any software or inappropriate material on to the network.

5.6 Staff will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.

5.7 Staff should understand that the right is reserved to remotely monitor and intercept network activity.

5.8 Staff are required to lock laptops if left unattended for any length of time, regardless of location, to prevent unauthorised access to sensitive material. This may be quickly done by pressing the Windows key and the 'L' key at the same time

6. Legislation

6.1 All network users are bound by current relevant legislation. The applicable laws (as amended) include, but are not limited to:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1998
- Criminal Justice Act 1988
- Defamation Acts 1952 and 1996
- Freedom of Information Act 2000
- Human Rights Act 1998
- Obscene Publications Act 1959 and 1964
- Protection of Children Act 1988
- Protection from Harassment Act 1997
- Public Order Act 1986
- Race Relations Amendment Act 2000
- Telecommunications Act 1984
- Data Protection Acts 1994 and 1998
- Sex Discrimination Act 1986
- Regulation of Investigatory Powers Act (RIPA) 2000

6.2 Staff should understand that any attempt to bypass the School, or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution.

6.3 Where it is believed that a member of staff is in breach of legislation appropriate action will be taken.

7. ICT Equipment and Suites

7.1 Staff may not move or authorise any person to move any ICT Equipment.

7.2 Staff may not pass on any ICT Equipment to any other person. It must first be passed back to the ICT Support department and then reissued.

7.3 Any equipment issued to staff remains the property of the school and must be returned upon request.

7.4 Upon termination of employment at the School all equipment must be returned.

7.5 Staff are responsible for all equipment issued to them and must take reasonable precautions to protect such equipment, including complying with insurance requirements of securing equipment at all times as detailed in the document 'Staff Laptop Loan Scheme'

7.6 Staff are responsible for all equipment and use of workstations by students during their lessons in ICT Suites. Their department will be billed for any associated damage.

7.7 No students may be allowed to use ICT Suites without first obtaining permission from a member of staff.

7.8 Staff members may not loan laptops etc. to family members/friends, neither shall user names/passwords be passed on to family/friends/

8. Additional Systems

8.1 Members of staff may have access to additional systems which include, but are not limited to: Finance Software, SIMS, Exam and Attendance Software. Access to these systems is granted only where necessary.

8.2 These systems require additional passwords. It is the responsibility of the member of staff to ensure that their password has basic complexity to it and that their password is only known by them.

8.3 IT or audio-visual equipment faults should be logged on the IT support site which is accessible via the staff intranet. In the event of a serious fault or an emergency, IT support can be contacted on extension 222.

9. Sanctions

In the event that this Acceptable Use Policy is breached, staff will be subject to sanctions which may include, but are not limited to:

- Disciplinary procedures;
- Temporary or permanent restriction of network access;
- Temporary or permanent revocation of network rights;
- Restriction to or denial of access to ICT Suites;
- Investigation under the Regulation of Investigatory Powers Act (RIPA) 2000.

Staff Agreement

I have read and understood the Staff Acceptable Use Policy for St Crispin's School.

I understand that should I be found in breach of the Acceptable Use Policy I may be liable to disciplinary procedures and, if appropriate, the Police and local authorities may become involved.

I accept that it is my responsibility to be aware of amendments to this Acceptable Use Policy which can be found on the School's Intranet under the Additional Policies section of the handbook.

Staff Name *		*** USE BLOCK CAPITALS**			
Staff Signature		**Date**	DD	MM	YY

School Agreement

(To be signed by authorised ICT Support department staff only)

I acknowledge the above named member of staff has returned a signed Acceptable Use Policy which signifies agreement to all clauses of the Acceptable Use Policy.

I therefore grant access to the Internet from the date below and permit access to the School's ICT Resources under the conditions of this Policy.

Staff Name *		*** USE BLOCK CAPITALS**			
Authorised Signature		**Date**	DD	MM	YY