e-Safety and Data Security Policy

a) This policy applies to all Trusts managed by Wootton Academy Trust (WAT)
b) This policy was adopted by WAT in **October 2017**
c) This policy was reviewed in October 2017
d) The next review is October 2018

Contents

Introduction

1. At Wootton Academy Trust we encourage student engagement with Information and Communication Technology (ICT) as we believe that it enables them to learn, communicate and explore the world in new ways. Many young people are now skilled in using computers, games consoles, mobile phones and tablet computers. However, with this new technology we also acknowledge that there are also new risks.

   We believe that everyone in our Trust community is responsible for the welfare and safety of children and it is therefore crucial that all stakeholders understand what these risks are and how we can all work together to enjoy these new technologies safely.

2. E-Safety is essentially about creating a safe environment when using ICT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber bullying, as well as detailing how we respond to e-safety issues when they emerge.

3. *"As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal."*[1]

   Our aim is to address these potential issues by regularly providing clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach, as outlined in this document; this will invariably involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

4. One of the key risks of using the internet, email or other social media platforms is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age inappropriate or biased. One of the key benefits of the web is that it is open to all but unfortunately this also means that for example, those with extreme political, racist, sexual or other prejudiced views are able to publicise those opinions.

5. In the case of pornography and indecent images of children, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development but young people may be shocked by some of the material online and it is not known what the long-term effects of exposure to such images may be. Seeking out some aspects of pornography is a criminal offence and could result in a criminal conviction.

[1] Safeguarding Children in a Digital World – Becta ICT Advice

6. The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies and is probably the risk most reported by the media. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these individuals is to establish and develop relationships with young people with the sole purpose of persuading them into relationships which can then progress to sexual activity. Child sex offenders will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. (Safeguarding Children in a Digital World. Becta 2006). Such behaviour is known as 'grooming'.

Roles and Responsibilities

7. As a school we see it as our responsibility to respond to e-safety concerns, irrespective of whether they occur inside or outside of school. Breaches to our school network protocols will be dealt with rapidly by our network manager in liaison, where appropriate, with the DSL and/or other relevant Year Leaders. However, where the school receives information of a safeguarding nature concerning online activity which has taken place outside school, the school is equally committed to engaging with the students concerned and their parents to resolve the situation. Where we feel there is an ongoing risk to a young person, Children's Services and occasionally the Police, may be contacted to provide further support. All information will be recorded on the CPOMs as per the Safeguarding and Child Protection Policy.

8. It is the responsibility of all members of our school community, including teaching and non-teaching staff, governors, volunteers and students, to prevent and tackle e-safety issues. In line with the school's Safeguarding and Child Protection Policy, all e-safety concerns should be shared at the earliest opportunity with the DSL or Early Help Officer and in any case before the end of the school day via CPOMs. The DSL is responsible for ensuring that technical staff are aware of what constitutes an e-safety concern which it would be necessary to report and undertake annual safeguarding training. The DSL will report regularly to the safeguarding governor on incidents of e-safety concerns and the subsequent actions and outcomes within the school.

9. The Executive Principal/Principal is responsible for ensuring that e-safety concerns are monitored and that staff remain appropriately trained to respond to such concerns. It is also the responsibility of the Executive Principal/Principal to ensure that preventative work is ongoing with students and that awareness raising among parents is ongoing.

Recognition and response

10. All members of our school community should be alert to the possibility that:

    - A child may already have been/be being abused and the images may have been distributed on the internet or by mobile telephone;
    - An adult or older child may be grooming a child for sexual abuse, including for involvement in making abusive images. This process can involve the child being shown abusive images;
    - An adult or older child may be viewing and downloading child sexual abuse images.

The risks posed by new technologies

11. As with many new or and emerging technologies, the internet has brought unfamiliar challenges, some of which create actual or potential dangers for children and young people.

12. New technologies have offered children and young people revolutionary advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. The main risks are in relation to sexual exploitation and the use of technology to bully and record physical abuse.

13. Some of the most common risks to children and young people are as follows:

    <u>Children viewing adult pornography</u>

    Children & young people often access adult pornography. However, the persistent viewing of material which is degrading, violent or sadistic or beyond the realms of normal curiosity can affect how young people can think about intimacy, themselves and their values and attitudes towards relationships and sexual development. Adult pornography can also be used by adults or young people as part of a grooming process.

    <u>Children abused through using the Internet and mobile phones</u>

    Technologies such as chat rooms, social media and SMS are often used by those wanting to sexually exploit children and young people. These perpetrators often exploit young people who are vulnerable by grooming them.

    Children can be coerced to take part in sexual activity online by abusers who employ specific conversational techniques. The grooming process is no different from that used by abusers offline. However, the whole abusive episode takes place online without physical contact between the child and perpetrator. The most common place for targeting these children is in social networking sites and chat rooms. When discovered, children will often deny any such activities, due to both the grooming process and the shame that many children feel when discovered doing something that have been told not to reveal and about which they feel deep humiliation and fear.

Young people creating and sending indecent images of themselves to others

Occasionally young people choose, or are coerced, into creating and sending indecent images of themselves to others. This can sometimes be vulnerable individuals who have been made to feel special and have been convinced that the other person involved loves them, is attracted to them. Often the other individual might promise to delete the images or to keep them secret. This can lead to considerable distress for the victim if the abuser then choses to publicise the images. It can also result in blackmail if the victim says no to creating and sending further, more explicit images.

Children, who create, view or download sexually abusive images of other children

Although some children plan to and purposefully download these images, others may have been forced to do so by peer group pressure or they may have been introduced to these sites by predatory adults as part of grooming for sexual abuse.

Young people creating or placing images of other young people online

The use of the internet as a tool for bullying is also becoming increasingly common. 'Happy slapping' and other recorded physical assaults, for example, can be carried out with the intention of humiliating, compromising or exploiting the young person who is the subject of the image.

Children groomed online for sexual abuse offline

It is an offence to groom a child. Sometimes children are befriended online by individuals with the sole purpose of gaining their trust. Often they may lie about their age and background to appeal to the young person, building up their trust until a point when they can suggest that they meet. While this is rare, research shows that in the UK, over eight million children have access to the internet and a significant proportion of these children (one in twelve) have met in person with someone who they first met online.

Children made the subject of child abuse images or pseudo-images

Children who are the subject of child abuse images may suffer incalculable trauma which may affect them for the rest of their lives. Perpetrators often use strategies to inhibit children disclosing the abuse: children may be shown abusive images of other children or their own abusive images in an attempt to normalise the activity; abusers may encourage children to place images of themselves or friends online; victims may be encouraged to be proactive in either their own sexual abuse or that of other children.

Pseudo images may be created of particular children by the technological manipulation of existing photographs, art or cartoons. These images often have the same impact on the victim as non-pseudo images.

Our response to e-safety risks to students

14. In all cases of e-safety concern, Wootton Academy Trust follows the school's Child Protection Policy to ensure concerns are reported appropriately as a matter of urgency and on the same day of a concern emerging, to the DSL or Early Help Officer. Where a risk is deemed to exist, parents, Children's Services and where appropriate, the Police will be informed. An assessment will usually be carried out by Children's Services to ensure that victims are fully protected and that the behaviour of child perpetrators is fully addressed.

15. Where it is felt that an ongoing risk is not a concern, the school is likely, usually following advice from Children's Services, to deal with the issues directly with students and their parents. This may involve meetings with students and parents whereby boundaries/ restrictions to internet access may be imposed. The school may choose to involve external agencies such as the Police or the Sexually Inappropriate Behaviour Service (SIBS) as a way of educating young people further about risk, online safety. For child perpetrators, this may involve work which focuses on respecting themselves and others.

16. Education is the key to minimising the online risks to students. PSHE sessions and assemblies throughout the year alongside aspects of the Computing curriculum throughout the year are used to educate students on appropriate online behaviour.

17. These sessions address the following:

- our approach to cyber bullying, with specific reference to our Anti Bullying Policy;
- the safe use of social media, including utilising privacy settings and the pitfalls of sharing personal information and photographs;
- the significance and consequences of their online behaviour, including digital footprints, legal sanctions and career prospects;
- online stranger danger, including how to recognise and report suspicious activity;
- the school's response to online behaviour that may bring the school or its members into disrepute.

18. The Child Exploitation and Online Protection Centre (CEOP, www.ceop.police.uk/safety-centre) brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse. A link to CEOP is available on the Student Welfare section of the school website.

Cyber-bullying

19. Bullying may be defined as deliberately hurtful behaviour, usually repeated over a period of time, where it is difficult for those bullied to defend themselves. It can take many forms but the main types are:

    - physical (e.g. hitting, kicking, theft)
    - verbal (e.g. racist or homophobic remarks, threats, name-calling)
    - emotional (e.g. isolating an individual from the activities and social acceptance of their peer group)

    "The damage inflicted by bullying (including cyberbullying via the internet) can frequently be underestimated. It can cause considerable distress to children, to the extent that it affects their health and development or, at the extreme, causes them significant harm (including self-harm). All settings in which children are provided with services or are living away from home should have in place rigorously enforced anti-bullying strategies." (Paragraph 11.57, Working Together 2010).

20. New technologies have offered children and young people innovative advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. Bullying through technology (cyber-bullying) can be devastating for the victim and unlike in the real world, the victim can be targeted at any time day or night, home or school.

21. Bullying can include emotional and/or physical harm to such a degree that it constitutes significant harm.

22. All staff at Wootton Academy Trust are aware of the need to be alert to cyber bullying and in line with our Anti Bullying Policy, staff are expected to report all instances of bullying, including racist and homophobic bullying, to their Year Leader or a member of the pastoral team, who will address these issues as a matter of urgency.

23. More serious cases of bullying or ongoing bullying following intervention should be discussed with the school's DSL and could involve making a referral to Children's Services. **Separate referrals for assessment and support may be made in respect of both child victim and child abuser.**

24. Where the bullying involves an allegation of crime (threats of assault, theft, harassment) a referral may be made to the police.

25. Information about good practice in anti-bullying strategies (real & virtual) for schools, can be accessed at; https://www.gov.uk/government/publications/the-use-and-effectiveness-of-anti-bullying-strategies-in-schools

Internet Usage

26. Ensuring internet use enhances learning
    - Internet access will be designed expressly for student use and will include filtering appropriate to students' ages
    - Students will be taught what is acceptable and what is not acceptable and given clear learning objectives when using the Internet
    - Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age
    - Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

27. Student evaluation of internet content
    - Any user discovering unsuitable sites must report the address and content to; the Internet Service Provider, the Network Manager, a teacher or the DSL as appropriate
    - The use of Internet derived materials must comply with copyright law
    - Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
    - Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

28. Management of email
    - Students may only use approved email accounts on the school system
    - Access in school to external personal email accounts will be blocked for students
    - Students must immediately tell a teacher if they receive offensive email
    - Students must not reveal details such as address/telephone number of themselves or others or arrange to meet anyone in email communication
    - Social email can interfere with learning and will be restricted
    - Email sent to an external organisation should be carefully written and authorised by a member of staff before sending
    - The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed
    - It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business
    - Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

29. Management of the school website content
    - The point of contact on the website should be the school address, email and telephone number. Staff and students' home information will not be published
    - Use of photographs showing students and students' names will not be used on the website without parental consent
    - The Senior IT Technician, acting as the Executive Principal/Principal's nominee, will take overall editorial responsibility and ensure that content is accurate and appropriate

- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained

30. Social networking
- Students will not be allowed access to public or unregulated chat rooms, social networking sites and forums
- Students may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised

31. Authorisation of internet access
- The school will maintain an up to date record of all staff and students who are granted Internet access
- All Internet access is monitored and recorded using electronic means
- All staff and students (and students' parents) must sign the Acceptable Use Agreement
- Inappropriate use of the Internet will be dealt with in accordance with the school's Behaviour Policy

32. Risk assessment
- Some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure such material is not accessed by students. However, it is not possible to guarantee that such material will never appear on a school computer – Wootton Academy Trust cannot accept liability for material accessed or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risk will be reviewed regularly

33. Internet filtering
- The school will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved
- The Trust uses 'Lightspeed', a Firewall software package, to filter internet content. This is run on a proxy in school. All internet traffic goes out through the Trust's Lightspeed system and so is filtered and monitored.
- The Network Manager will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable.
- Any Internet user must report unsuitable/illegal sites to the Network Manager (and the DSL if necessary) immediately
- Students and staff who attempt to access a blocked site are informed by a Lightspeed or Impero screen message. Additionally, the Acceptable Use Agreement includes statements on logging and monitoring of school ICT equipment.
- If filtered websites need to be used by staff, they must inform ICT Technicians to have them unblocked for a set period of time.
- User logs are reviewed daily by a member of the Network team and any issues of concern are referred to the DSL or Year Leaders.

34. Student, staff and parental awareness
    - All stakeholders will be made aware of this policy and how it relates to them
    - All staff will sign the Acceptable Use Agreement
    - All students will sign the Acceptable Use Agreement – countersigned by parents
    - Students will be instructed in responsible and safe internet use before being granted access
    - Responsible use of the internet, including social networking will be discussed through the PSHE and the Computing curriculum (including online safety and sexting), covering use in school and outside of school. Please refer to AT Safeguarding and Child Protection Policy – Appendix 4.
    - The monitoring of internet use is a sensitive matter – staff who operate monitoring procedures will be supported by the Network Manager and responsible Assistant Principal.
    - Staff training in safe and responsible internet use and on the contents of this policy will be provided as required
    - A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available.

35. Cases of internet misuse and other disciplinary breaches related to the policy will be dealt with through the school's Behaviour, Anti-Bullying and Safeguarding and Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel.

IT Systems

36. **ICT System Security**
    - The Trust's ICT systems will be reviewed regularly with regard to security
    - Virus protection will be installed and updated regularly
    - Files held on the school's network will be regularly checked
    - Use of portable media such as memory sticks and CD will be reviewed regularly
    - Downloading of unauthorised files will be prohibited, and where possible blocked
    - Use of the school's ICT systems will be subject to the Data Protection Act and the Computer Misuse Act

37. **Infrastructure –** Procedures are in place to protect the school and its students from a malicious cyber-attack. All computer equipment is protected by the security of the school. All external doors to buildings are locked. Visitors to the site are booked in. Servers, PBX and network storage are kept in locked rooms with restricted access. Network communications equipment is kept in locked cabinets. The school network is protected behind the firewall to protect from external malicious attack.

    Access to Servers and Network is limited to a few school technical staff and an external support engineer (from XMA when necessary). Individual user ids are used and are protected with strong passwords.

    All user data and servers are backed fully at the weekend and removable storage backup taken to alternative locations. An incremental backup of user data and servers is taken each weekday.

The school uses VLANs to separate curriculum and administration networks, restricting activity and access as appropriate.

38. **Downloading software –** In order to prevent unauthorised users downloading software on school devices, laptops and desktop PCs are protected by user names and passwords. Students are automatically blocked from downloading software and virus guards are installed so that staff who download software can do so safely.

39. **Passwords and security –** Access to school networks and devices is controlled through careful password procedures, whereby students are taught about password strengths in their ICT lessons, before setting strong passwords of at least six characters which include upper and lower case letters as well as either a symbol or a number. Additionally, each user has a home folder on the server which cannot be accessed by other users. Students and staff also have access to their own designated shared areas which contain resources.

    School IT induction for staff ensures that they are briefed on the dangers of viruses and attachments.

    Staff are encouraged to ensure that they lock their screen before moving away from their computer during your normal working day to prevent unauthorised access.

40. **External service providers –** The school is cautious in using external internet services and as such, for third party vendors, it is required that any internet access for students is only provided through the school's internet filter and monitoring software.

41. **Guest access –** Procedures are in place to provide internet access to temporary staff such as trainee teachers, through temporary user IDs. Guest Wi-Fi is available to allow guest access to the internet using the same filtering system as other Trust users.

42. **Monitoring -** user logins, user printing, internet access and inappropriate activity on PCs and laptops are all monitored and reported to the appropriate school leader if concerns arise. Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please contact the network team.

    ICT authorised staff may monitor, intercept, access, inspect, and disclose e-mails, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

    ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

43. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Related documents and timescales

44. This policy should be read in conjunction with the following policies and procedures:

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Social Media Policy
- Whistleblowing Policy

45. This policy will be reviewed annually following consultation with students, relevant staff and governors.

Further guidance and support

For professionals:

- The UK Council for Child Internet Safety (UCCIS) www.education.gov.uk/ukccis brings together over 160 stakeholders from across the internet safety spectrum who have come together to work in collaboration for the good of children and families.

- The Child Exploitation and Online Protection Centre (CEOP, www.ceop.police.uk brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24-hour online facility for reporting instances of online child sexual abuse.

- www.thinkuknow.co.uk – a website for professionals (and children, young people and parents) full of information and resources about staying safe online.

- https://www.iwf.org.uk - This is an organisation, which works with the Police and Internet Service Providers to trace those responsible for putting harmful or illegal material on the web. It also encourages web surfers who find harmful or illegal material to report it.

For children, young people and their carers:

The following information gives advice to parents and children in terms of considering the dangers and managing risks, as well as information about computer software and supervised chat rooms etc.

- www.thinkuknow.co.uk – a website for children, young people, parents and professionals full of information about staying safe online.

Appendix 1 - Social Media Guidelines

Introduction

For the purposes of these guidelines, social media refers to any interactive Web 2.0 platform, including social networks, internet forums and blogs. Given the rapid expansion of social media, it is impossible to list all possible types of media. Staff should assume that all online activity is covered by this policy. Employees should follow these guidelines in relation to any social media that they use, both at work and at home.

Scope

These guidelines apply to teachers, support staff, governors, volunteers and all who work on the school site.

It takes account of all the appropriate legislation and sets out to:

- Assist those who work with pupils to work safely and responsibly, to monitor their own standards of behaviour and to prevent the abuse of their position of trust with pupils.
- Offer a code of practice relevant to social media for educational, personal and recreational use.
- Advise that, in the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken if necessary in order to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with pupils.

This policy should be read in conjunction with the school's use of IT policy.

Use of social media in the school

Staff are not permitted to access social media websites from the school's computers or other school device at any time unless authorised to do so by a member of the senior leadership team. Staff are discouraged from using their own devices to access social media websites while they are in school, outside of lessons or other structured sessions unless this is for school-related business. Excessive use of social media, which could be considered to interfere with productivity, will be considered a disciplinary matter.

Staff should assume that anything they write (regardless of their privacy settings) could become public so should ensure that they are professional, maintaining a clear distinction between their personal and professional lives.

Any use of social media made in a professional capacity must not:

- Bring the school into disrepute.
- Breach confidentiality.
- Breach copyrights of any kind.
- Bully, harass or be discriminatory in any way.
- Be defamatory or derogatory.

Use of social media outside of school

The school appreciates that staff may make use of social media in a personal capacity. However, staff must be aware that if they are recognised from their profile as being associated with the school, opinions they express could be considered to reflect the school's opinions and so could damage the reputation of the school. For this reason, staff should avoid mentioning the school by name, or any member of staff by name or position. Opinions should follow the guidelines above so as not to bring the school into disrepute, breach confidentiality or copyright, or bully, harass or discriminate in any way.

General considerations

When using social media staff and others should:

- Never share work log-in details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses to pupils or parents.
- Restrict access to certain groups of people on their social media sites and pages.

Those working with children have a duty of care and are therefore expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and pupils both within and outside of school. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties for 'cyber-bullying', for example, or identity theft.

Staff should not make 'friends' of pupils at the school because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any pupils.

Staff should also carefully consider contact with a pupil's family members because this may give rise to concerns over objectivity and/or impartiality.

Staff should keep any communications with pupils transparent and professional and should only use the school's systems for communications.

If there is any doubt about whether communication between a pupil/parent and member of staff is acceptable and appropriate a member of the senior leadership team should be informed so that they can decide how to deal with the situation.

Before joining the school, new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Disciplinary action

Any breach of this policy may lead to disciplinary action under the school's disciplinary policy. Serious breaches of this policy, such as incidents of bullying or of social media activity causing damage to the organisation, may constitute gross misconduct and lead to dismissal.

Appendix 2 - Acceeement

WOOTTON
ACADEMY TRUST

Wootton Academy Trust: Acceptable Use Agreement for Student Users

Introduction and points to note

As part of our students' learning experience and the development of ICT skills, Wootton Academy Trust is providing our students with a computer network account and access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached **Acceptable Network and Internet Usage Agreement** and sign and return the consent form so that your child may use computers and the Internet within the Trust.

Code of Conduct:

1. I **will not** share my passwords with anyone.
2. I **will** only use, move and share securely data/files that I own.
3. I **will** make sure all messages I send are respectful, using appropriate language.
4. I **will not** use my mobile device during lesson time unless I am given permission.
5. I **will** always keep my personal details private (my name, school name and address, home address any contact numbers, family information etc…).
6. I **will** only use an e-mail accounts that have been approved by my school.
7. I **will not** buy or order goods online without a teacher's permission.
8. I **will** only use, create and share content that is legal.
9. I **understand** that any illegal activity that I conduct on the school network may be reported to external agencies.
10. I **will** not install any programs, or store any personal data (e.g. mp3, personal pictures) in my school user area.
11. I **will** respect copyright and the intellectual property rights of others.
12. I **will not** use Internet facilities to advertise for personal gain.
13. I **understand** that any of my files can be viewed by ICT support staff and other members of staff, and that any files considered inappropriate may be deleted, and that this could lead to further disciplinary procedures.
14. I **will not** interfere with any ICT equipment (e.g. cables, mouse etc…)
15. I **will** only print final copies of work, unless given permission to do otherwise by a member of staff.
16. I **understand** that Wootton Academy Trust may monitor my use of the systems, devices and digital communications.

E-safety

The following guidelines apply while using Wootton Academy Trust equipment and ICT network: -

1. I **will not** visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    a. Any form of extremism
    b. Promoting racial or religious hatred.
    c. Any form of pornography (including sexting)
    d. Promoting discrimination of any kind.
    e. Promoting violence or bullying.
    f. Promoting illegal acts.
    g. Breaching any of my school's Internet filters
    h. Anything which exposes others to danger.
    i. Information that may be offensive to others.
    j. Chain letters.
    k. Breaches of copyright law.
    l. Using personal technology for taking/transferring images of students or staff without permission.
2. I **will** only visit sites which are appropriate and not blocked by the schools' filtering system, and adhere to the sites' terms and conditions. Access to social media accounts (e.g. facebook, instagram), video streaming websites (e.g. Netflix) is strictly prohibited without permission from a teacher and a member of the network team.
3. I **will** make sure I know where to find and how to use the CEOP report abuse button.
4. I **know** that anything I share online may be monitored.
5. I **know** that once I share anything online it is out of my control and can be used or changed by others.
6. I **will** report unsuitable or uncomfortable content, activities or e-mails to a member of staff

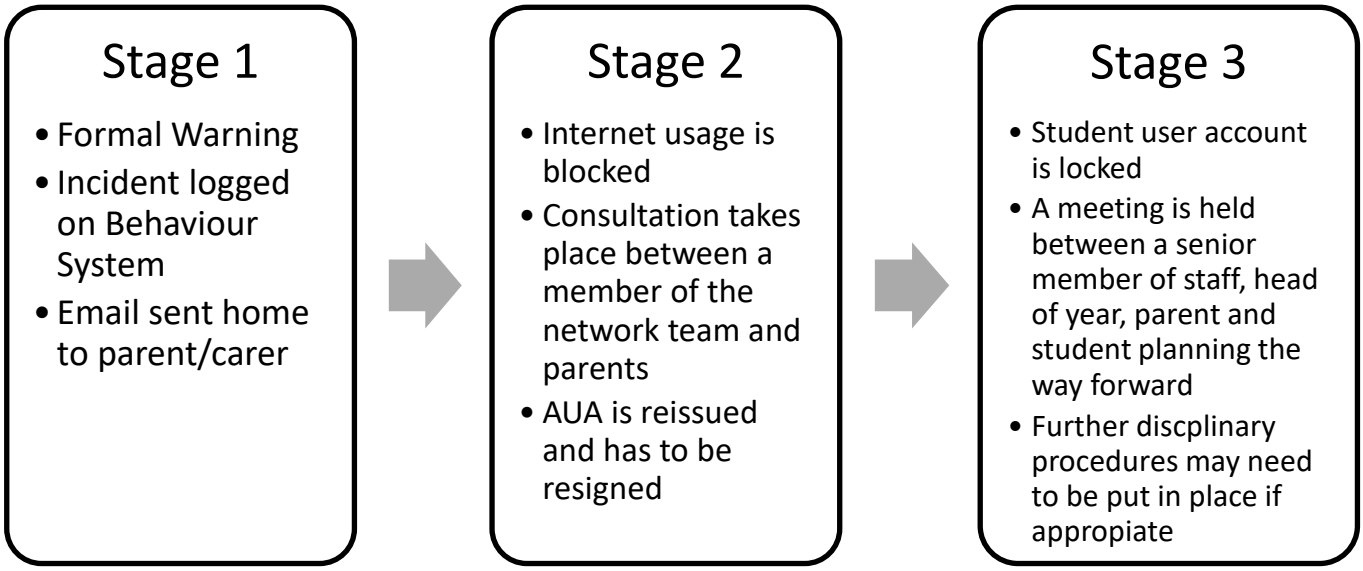
Advice

Both at home and at school we advise:

1. You **do not** upload pictures or digital images of yourself or others without a responsible adult's permission.
2. You **only** communicate electronically with people you know or have been approved by my school.
3. You **never** meet an online friend or contact without taking a responsible adult that you know with you.
4. You ensure that any social networking profiles you may have are set to private.

Sanctions

Where the acceptable use agreement has not been followed, the following sanctions will be implemented



Note: Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour. When applicable, police or local authorities may be involved.

User Agreement Reply Slip

I have read and I understand the school Rules for Acceptable Network and Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Name			
Year and Tutor Group			
Student signature		**Date**	

Having parental responsibility for the student signing above, I grant permission for my son or daughter to access networked computer services such as electronic mail and the Internet. I understand that some materials on the Internet may be objectionable, but I accept responsibility for my daughter or son to follow the above stated rules

Parent/Guardian Signature		**Date**	

***Please return to Network Office, at Wootton Upper School or Kimberley College*.**