Policy Type: General

National Minimum Standards Requirement:

DfE Requirement:

Governor Authorised: RC & SC

Staff/Student Receipt: All

Availability: Policy Handbook

 Staff Drive/Staff Communal/ New College Policies

 Policy Co-ordinator

POLICY NO

**163**

**NEW COLLEGE WORCESTER**

**E-SAFETY POLICY**

**NCW E-Safety Policy Contents**

A.1.1 Responsibilities: the E-Safety Committee

A.1.2.a Responsibilities: E-Safety Co-ordinator

A.1.2.b Responsibilities: Member of SLT with responsibility for E-Safety

A.1.3 Responsibilities: Governors

A.1.4 Responsibilities: Principal

A.1.5 Responsibilities: Academic and Care Staff

A.1.6 Responsibilities: IT Technician

A.2.1 Policy Development, Monitoring and Review

A.2.2 Policy Scope

A.2.3 Acceptable Use Agreements

A.2.4 Self Evaluation

A.2.5 Whole College Approach and Links to Other Policies

A.2.6.a Inappropriate or Illegal Activities and Sanctions – General Statements

A.2.6.b Inappropriate or Illegal Activities and Sanctions – Students

A.2.6.c Inappropriate or Illegal Activities and Sanctions – Staff

A.3.1 Use of Hand Held Technology (Personal Phones and Other Hand Held

 Devices)

A.3.2 Use of Communication Technologies

A.3.2a E-mail

A.3.2b Social Networking (taken and adapted from General Teaching Council

 Scotland)

A.3.3 Use of Digital and Video Images

A.3.4 Use of Web-Based Publication Tools

A.3.4a Website

A.3.5 Professional Standards for Staff Communication

Section B. Infrastructure

B.1 Password security

B.2.1 Filtering

B.2.1.a Introduction

B.2.1.b Responsibilities

B.2.1.c Education/training/awareness

B.2.1.d Changes to the filtering system

B.2.1.e Monitoring

B.2.1.f Auditing/reporting

Section C. Education

C.1.1 E-Safety Education

C.1.2 Information Literacy

C.1.3 The Contribution of the Students to the E-Learning Strategy

C.2 Training

Section D

D Appendix 1 Acceptable Use Agreements and Signature Slip

D Appendix 2 E-Safety Curriculum

D Appendix 3 Supporting Resources and Links

D Appendix 4 Glossary of Terms

**A.1.1 Responsibilities: the E-Safety Committee**

NCW has an E-Safety committee led by our E-Safety Co-ordinator and made up of staff, students and the E-Safety Governor. It meets on a twice-termly basis to:

* Review and monitor this E-Safety Policy.
* Consider any issues relating to school filtering (see section B.2.1 of this policy).
* Discuss any E-Safety issues that have arisen and how they should be dealt with.

Issues that arise are referred to other NCW bodies as appropriate and, when necessary, to bodies outside the establishment, such as the Worcestershire Safeguarding Children Board.

**A.1.2.a Responsibilities: E-Safety Co-ordinator**

The NCW E-Safety Co-ordinator is the person responsible to the Principal and Governors for the day to day issues relating to E-Safety.

The E-Safety Co-ordinator:

* leads the E-Safety Committee
* takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing NCW’s E-Safety policies.
* ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident
* provides training and advice for staff
* liaises with NCW IT technical staff
* meets regularly with E-Safety Governor to discuss current issues and review incident logs
* reports regularly to Senior Leadership Team
* receives appropriate training and support to fulfil their role effectively

**A.1.2.b Responsibilities: Member of SLT with Responsibility for E-Safety**

The member of SLT with responsibility for E-Safety:

* receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments
* meets IT staff half-termly to review the output of monitoring software
* attends relevant meetings and committees of the Governing Body

**A.1.3 Responsibilities: Governors**

Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Residential Care and Safeguarding Committee of the Board of Governors, receiving regular information about E-Safety incidents and monitoring reports.

A member of the Governing Body has the role of E-Safety Governor which involves regular meetings with the E-Safety Co-ordinator and Designated Safeguarding Lead termly, prior to each meeting of the Residential Care and Safeguarding Committee, with an agenda based on:

* monitoring of E-Safety incident logs
* reporting to the Residential Care and Safeguarding Committee of the Governing Body

**A.1.4 Responsibilities: Principal**

* The Principal is responsible for ensuring the safety (including E-Safety) of all members of the NCW community, although the day to day responsibility for E-Safety is delegated to the E-Safety Co-ordinator
* The Principal and another member of the Senior Leadership Team will be familiar with the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff, including non-teaching staff. (see flow chart on dealing with E-Safety incidents (included in section 2.6 below) and other relevant disciplinary procedures).

**A.1.5 Responsibilities: Academic and Care Staff**

Academic and Care Staff are responsible for ensuring that:

* they safeguard the welfare of students and refer safeguarding concerns using the proper channels: this duty is on the individual, not NCW.
* they have an up to date awareness of E-Safety matters and of the current NCW E-Safety Policy and practices.
* they have read, understood and signed NCW’s Acceptable Use Agreement for staff (see Appendix 1).
* they report any suspected misuse or problem to the E-Safety Co-ordinator or the member of SLT with responsibility for E-Safety.
* they undertake any digital communications with students in a fully professional manner and only using official systems (see A.3.5).
* they embed E-Safety issues in the curriculum and other activities, also acknowledging the planned E-Safety Programme (see section C).

**A.1.6 Responsibilities: IT Technician**

The ICT Technician is responsible for ensuring that:

* NCW’s ICT infrastructure and data are secure and not open to misuse or malicious attack.
* NCW meets the E-Safety technical requirements outlined in section B.2.2 of this policy.
* shortcomings in the infrastructure are reported to the IT Team Leader or Principal so that appropriate action may be taken.

**A.2.1 Policy Development, Monitoring and Review**

This E-Safety Policy has been developed by a working group made up of:

E-Safety Coordinator

Designated Safeguarding Lead

Deputy Head of Care

IT Team Leader

Assistant Principal: Business and Finance

Consultation with NCW has taken place and adopted by the Governing Body on 19/07/17 (Governors) and 07/11/17 (RC & SC)

**Schedule for Development, Monitoring and Review of this Policy**

This E-Safety Policy was approved by the Governing Body on:

The implementation of this E-Safety Policy will be monitored by the Residential Care and Safeguarding Committee of the Governing Body

Monitoring of this policy will take place annually.

The Residential Care and Safeguarding Committee of the Governing Body will receive regular reports on the implementation of the E-Safety Policy generated by the E-Safety Group (which will include anonymous details of E-Safety incidents) as part of a standing agenda item with reference to Safeguarding*,* once per term.

The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of technology, new threats to E-Safety or incidents that have taken place.

Should serious E-Safety incidents take place, the following external persons / agencies may be informed: Worcestershire Safeguarding Children Board, the relevant Local Authority Designated Officer, West Mercia Police. See section A.2.6 Illegal or inappropriate activities and related sanctions.

**A.2.2 Policy Scope**

This policy applies to all members of the NCW community, (including academic, care and support staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of NCW’s IT systems, both in and out of the establishment.

The Education and Inspections Act 2006 empowers Principals, to such extent as is reasonable, to regulate the behaviour of students when they are off the NCW site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other E-Safety incidents covered by this policy, which may take place out of NCW, but are linked to members of the NCW community.

NCW will deal with such incidents using guidance within this policy as well as associated behaviour and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate E-Safety behaviour that take place out of NCW.

**A.2.3 Acceptable Use Agreements**

All members of the NCW community are responsible for using the NCW IT systems in accordance with the appropriate Acceptable Use Agreement (AUA), which they will be expected to sign before being given access to College systems.

Acceptable Use Agreements are provided in Appendix 1 of this policy for:

* Students
* Staff (and volunteers)
* Parents/carers

Acceptable Use Agreements are introduced at parents’ induction meetings and signed by all students as they enter NCW. Parents re-sign the Agreement if circumstances demand it. Parents should notify NCW if this is the case.

All employees and volunteers of NCW sign when they take up their role and in the future if significant changes are made to the policy.

Parents sign once when their child enters NCW. The parents’ policy also includes permission for use of their child’s image (still or moving) by NCW, permission for their child to use NCW’s IT resources (including the internet) and permission to publish their work.

Induction policies for all members of the NCW community include this guidance.

**A.2.4 Self Evaluation**

Evaluation of E-Safety will take place as part of the regular NCW cycle of self-evaluation and improvement planning.

**A.2.5 Whole College Approach and Links to Other Policies**

This policy links to other NCW policies as follows:

**Core IT Policies**

IT Policy:

Data Security Policy

Acceptable Use Policy

Temporary Loan of College Equipment Policy

**Other Policies Relating to E-Safety**

Anti-bullying

PSCHE

Safeguarding

Behaviour

Use of images

Additional information, including Guidance for reviewing Internet sites and Criteria for website filtering, is held by the IT department

**A.2.6.a Inappropriate or Illegal Activities and Sanctions – General Statements**

NCW believes that the activities listed below are inappropriate in College (those in bold are illegal) and that users should not engage in these activities when using NCW equipment or systems (in or out of College).

Definition of offensive material: Material which promotes any kind of discrimination, racial or religious hatred; threats including physical violence or mental harm, or material which reasonable users find offensive.

Users shall not visit Internet sites, make, post, download, upload, transfer data, communicate or pass on material, remarks, proposals or comments that contain or relate to:

* **Child sexual abuse images (illegal - The Protection of Children Act 1978).**
* **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003).**
* **Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008).**
* **Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986).**
* Pornography.
* Promotion of any kind of discrimination.
* Promotion of racial or religious hatred.
* Threatening behaviour, including promotion of physical violence or mental harm .
* Any other information which may be offensive to colleagues or breaches the integrity of the ethos of NCW or brings NCW into disrepute.

Additionally the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the NCW:

* Using College systems to undertake transactions pertaining to a private business.
* Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by NCW.
* Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions.
* Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords).
* Creating or propagating computer viruses or other harmful files.
* Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files that causes network congestion and hinders others in their use of the internet).
* On-line gambling and non-educational gaming during working hours.
* On-line shopping/commerce during working hours, unless directly related to College business.
* Use of social networking sites during working hours, unless it is part of a role, (other than sites otherwise permitted by the College).

Note: it is permitted to share social media posts by NCW official accounts during working hours if appropriate.

If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

Please see Appendix 2. Members of staff are obliged to report such suspicions to the E-Safety Co-ordinator or, if illegal, the Principal.

It is more likely that NCW will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the NCW community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as indicated on the following pages.

|  |  |  |  |
| --- | --- | --- | --- |
| **A.2.6.b Inappropriate or Illegal Activities and Sanctions - Students** | **Refer to:** | **Inform:** | **Action:** |
| **Student sanctions** ***Unless staff feel that there are Safeguarding implications in which case the Designated Safeguarding Lead should be informed, incidents should be referred to the form tutor, senior houseparent or the E-Safety co-ordinator who will escalate appropriately.***  | **Form teacher /class teacher/key worker** | **E-Safety coordinator** | **Refer to Principal** | **Refer to LA** | **Refer to Police** | **Refer to Head of IT for action re filtering / security**  | **Parents / carers** |  **Remove of network / internet access rights** | **Warning** | **Further sanction**  |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** | **✔** | **✔** | **✔** | **✔** | **✔** | **✔** | **✔** | **✔** | **✔** | **✔** |
| **Unauthorised use of non-educational sites during lessons** | **✔** |  |  |  |  | **✔** |  |  |  |  |
| **Unauthorised use of mobile phone / digital camera / other handheld device** | **✔** |  |  |  |  |  | **✔** | **✔** |  |  |
| **Unauthorised use of social networking / instant messaging / personal email either on NCW or personal devices** | **✔** | **✔** |  |  |  | **✔** | **✔** |  | **✔** |  |
| **Allowing others to access the NCW network by sharing username and passwords** | **✔** | **✔** | **✔** |  |  | **✔** |  | **✔** | **✔** |  |
| **Attempting to access the NCW network, using another pupil’s account** | **✔** |  |  |  |  | **✔** |  | **✔** |  |  |
| **Attempting to access or accessing the NCW network, using the account of a member of staff** | **✔** |  | **✔** | **✔** |  | **✔** | **✔** |  | **✔** | **✔** |
| **Corrupting or destroying the data of other users** | **✔** | **✔** | **✔** |  |  | **✔** | **✔** | **✔** | **✔** |  |
| **Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature** | **✔** | **✔** | **✔** |  |  | **✔** | **✔** | **✔** | **✔** |  |
| **Continued infringements of the above, following previous warnings or sanctions** | **✔** | **✔** | **✔** | **✔** |  |  | **✔** | **✔** |  | **✔** |
| **Actions which could bring NCW into disrepute or breach the integrity of the ethos of NCW** | **✔** |  | **✔** | **✔** |  |  |  |  | **✔** |  |
| **Using proxy sites or other means to subvert NCW’s filtering system** | **✔** | **✔** | **✔** | **✔** |  | **✔** | **✔** | **✔** | **✔** |  |
| **Accidentally accessing offensive or pornographic material and failing to report the incident** | **✔** | **✔** |  |  |  | **✔** | **✔** |  |  |  |
| **Deliberately accessing or trying to access offensive or pornographic material** | **✔** | **✔** | **✔** |  |  | **✔** | **✔** | **✔** |  | **✔** |
| **Being knowingly in receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act**21 | **✔** |  | **✔** |  |  | **✔** |  | **✔** |  |  |

A.2.6.c Inappropriate or Illegal Activities and Sanctions - Staff

|  |
| --- |
|  |
| Staff sanctions | Line manager  | Principal | Police | Warning | Suspension | Disciplinary action |
| **Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).** |  | ✔ | ✔ |  | ✔ | ✔ |
| Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email | ✔ | ✔ |  | ✔ |  |  |
| Allowing others to access College network by sharing username and passwords or attempting to access or accessing the College network, using another person’s account | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Careless use of personal data e.g. holding or transferring data in an insecure manner | ✔ | ✔ |  | ✔ |  | ✔ |
| Deliberate actions to breach data protection or network security rules | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Corrupting or destroying the data of other users or causing deliberate damage to hardware or software |  | ✔ |  |  | ✔ | ✔ |
| Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Actions which could compromise the staff member’s professional standing  | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Actions which could bring NCW into disrepute or breach the integrity of the ethos of NCW | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Using proxy sites or other means to subvert NCW’s filtering system | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Accidentally accessing offensive or pornographic material **and failing to report the incident** | ✔ | ✔ |  | ✔ | ✔ |  |
| **Deliberately** accessing or trying to access offensive or pornographic material | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ |
| Breaching copyright or licensing regulations | ✔ | ✔ |  | ✔ | ✔ | ✔ |
| Continued infringements of the above, following previous warnings or sanctions | ✔ | ✔ |  | ✔ | ✔ | ✔ |

**A.3.1 Use of Hand Held Technology (Personal Phones and Other**

 **Hand Held Devices)**

We recognise that the area of mobile technology is rapidly advancing and it is NCW’s policy to review its stance on such technology on a regular basis.

Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

* Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances.
* Members of staff are free to use these devices outside teaching time.

An NCW mobile phone is available for staff to use on off-site activities should they request it.

Students are allowed to use their devices in class only when appropriate and instructed by the teacher.

**It should not be assumed that all students have access to hand-held devices**

A number of such devices are available in school and are used by students as considered appropriate by members of staff.

**Use of students’ personal devices which are connected to networks other than the NCW network**

Every student is entitled to have one device to use on our network and should obtain permission for any further devices. Students are not allowed to use their own device at NCW unless it has had content management software installed.

**A.3.2 Use of Communication Technologies**

**A.3.2a – E-mail**

Email is available to all members of the NCW community through the NCW network.

NCW’s official e-mail services may be regarded as safe and secure and are monitored.

Staff and students should use only the NCW e-mail services to communicate with others regarding NCW business when in the College, or on the NCW system by remote access.

Users need to be aware that e-mail communications may be monitored

Students normally use only a college e-mail account to communicate with people outside NCW and with the permission/guidance of a member of staff.

A structured education program is delivered to students which helps them to be aware of the dangers of and good practices associated with the use of e-mail (see section C of this policy).

Users must immediately report to their teacher or key worker/E-Safety Co-ordinator – in accordance with this policy (see sections A.2.6 and A.2.7) - the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such e-mail and should not delete it.

**A.3.2b Social Networking (Taken and Adapted from General Teaching**

 **Council Scotland)**

All staff at NCW are individuals with private lives, however, off-duty conduct matters and may have bearing on their professional life. Therefore sound judgement and due care should be exercised as conduct which may not directly relate to students may be relevant to a staff member’s fitness to work.

Notes:

* Normal disciplinary sanctions will be applied if a member of staff breaches these guidelines.
* It may be necessary for members of staff to join particular groups as part of their role, but this should be approved by the Principal.
* If members of staff want to tweet on behalf of NCW with an NCW Twitter account, they must be appointed by the Principal and the Marketing Manager and receive training. Tweets will be monitored and Quality Assured.

**Professional Vulnerability**

Members of staff can be vulnerable to unintended misuses for electronic communication. E-mail, texting and social media encourage casual dialogue and very often, very innocent actions can easily be misconstrued or manipulated. Electronic messages are not anonymous and can be tracked and stay permanently on the internet. Social media sites archive content posted, even when deleted from online profiles. Once information is placed on line, the author relinquishes control of it.

NCW staff should:

* always maintain a formal and courteous and professional tone in communicating with students and ensure that professional boundaries are maintained;
* only use official channels of communication ie NCW’s e-mail addresses and be aware of and comply with employer’s policies and guidance;
* not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with students;
* firmly decline student-initiated ‘friend’ requests from current and former students, unless the student is over eighteen years of age and has left at least two years previously. Staff should also decline requests from parents and not instigate any themselves. It is acceptable to decline such invitations and remind parents of more formal channels which they can discuss their child’s education;
* operate online in a way in which would not call into question your position as a professional, and not combine personal and professional posts under one account
* realise that students will be naturally curious about your personal life outside school and may try to find out more about you.
* Manage your privacy setting and keep them under review. These are particularly important with regard to photos, and remember that no privacy mechanism is 100% guaranteed;
* ensure your settings prohibit others from tagging you in any photos or updates without your permission and you can ask others to remove any undesirable content related to you;
* be aware that potential employers may view your online social media profiles;
* consider that conversations held online may not be private. Be aware of who may have access to what you post;
* assume that information you post can be accessed and altered;
* not discuss students, colleagues, parents or carers online or criticise your employer or others within the school community;
* respect pupil privacy and confidentiality at all times;
* Under the PREVENT duty for schools, staff should be aware of the importance of promoting British Values. Many groups with radical and extreme views post information on to social media and staff should avoid ‘following’ or ‘liking’ these groups. Staff have to be careful as many right wing groups use iconic imagery which seems harmless when they are first uploaded, however ‘liking’ specific posts could result in staff having other racist posts on their timeline. It is important to be cautious of information you support and share on social media.
* use strong passwords and change them regularly. Protect your mobile phone/smart phone/tablet computer with a PIN, especially when in school to protect access to its content and potential misuse;
* bring the matter to the attention of your employer using the proper procedures, if you are the victim of cyber bullying or uncomfortable with comments, photos or posts made by students of or about you.

**A.3.3 Use of Digital and Video Images**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. (See section C). In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

15

* Members of staff are allowed to take digital still and video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images. Those images should only be captured using College equipment; **the personal equipment of staff should not be used for such purposes.**
* Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or NCW into disrepute.
* Some students do not have permission for their digital/video image to be shared. Staff should check the relevant data in SIMS before taking and publishing digital/video images and ensure that images of such students are not shared or published.
* Students must not take, use, share, publish or distribute images of others without their permission and the E-safety curriculum should include this aspect.

See also the following section (A.3.4) for guidance on publication of photographs

**A.3.4 Use of Web-Based Publication Tools**

**A.3.4a – Website**

NCW uses [www.ncw.co.uk](http://www.ncw.co.uk) only for sharing information with the community beyond NCW. This includes, from time-to-time, celebrating work and achievements of students. All content is published by the Marketing Officer, not by individual members of staff, using the following guidelines:

* Personal information will not be posted on the NCW website and only official e-mail addresses will be used to identify members of staff (never students).
* Detailed calendars will not be published on the College website.
* Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with the following good practice guidance on the use of such images:
	+ students’ full names will not be used anywhere on a website or blog, and never in association with photographs.
	+ where possible, photographs will not allow individuals to be recognised.
	+ written permission from parents or carers will be obtained before photographs of students are published on the College website (see section A.2.3 and Appendix 1).
* Students’ work can only be published with the permission of the student and parents or carers. (see section A.2.3 and Appendix 1).

**A.3.5 Professional Standards for Staff Communication**

Teachers are governed by clear professional standards. Although the 2012 revised standards contain no specific references to ICT, there are particular codes of conduct that relate to E-Safety, as well as more generally. It is the College’s responsibility to act in the best interests of the students it serves, and that is what this section of the policy covers. The policy statements also need to ensure that the professionalism of teachers is preserved and that the integrity is not compromised.

In all aspects of their work at NCW, staff abide by the broad Professional Standards for Teachers laid down by the TDA effective from September 2012: <http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf>.

Teachers translate these standards appropriately for all matters relating to E-Safety.

Any digital communication between staff and students or parents / carers (e-mail, chat, learning platform, etc) must be professional in tone and content.

* These communications may only take place on official (monitored) College systems.
* Personal e-mail addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of students are used to inform this process also.

# **Section B. Infrastructure**

## B.1 Password security

The New College Worcester's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of New College Worcester (see section C of this policy)

## B.2.1 Filtering

New College Worcester receives filtering via JANET (ISP) at a very high level and through in house filtering via WatchGuard. This is intended to prevent users accessing material that would be regarded as illegal and / or inappropriate in an educational environment. Because the content on the web changes dynamically and new technologies are constantly being developed, it is not possible for any filtering service to be 100% effective. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use.

As the use of the internet continues to become more widespread and accessed through a wider range of technologies, users become more sophisticated in their internet use, therefore New College Worcester need continually to review their filtering and monitoring policies.

B.2.1a Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. No filtering system can, however, provide a 100% guarantee that it will do so. It is therefore important that the New College Worcester has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in New College Worcester.

It is recognised that New College Worcester takes full responsibility for filtering of content delivered to devices connected to its infrastructure.

### B.2.1b Responsibilities

The day-to-day responsibility for the management of the New College Worcester’s filtering policy is held by the e-safety coordinator (with ultimate responsibility resting with the principal and governors). They manage filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the New College Worcester filtering service must:

* be logged in change-control logs by the person making the change
* be reported to, and authorised by, a second responsible person prior to changes being made

All users have a responsibility to report immediately to teachers / e-safety coordinator any infringements of the filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

### B.2.1c Education / training / awareness

Pupils are made aware of the importance of filtering systems through the New College Worcester’s e-safety education programme (see section C of this policy).

Staff users will be made aware of the filtering systems through:

* signing the Acceptable Use Agreement (as part of their induction process)
* briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the New College Worcester’s filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

### B.2.1d Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at New College Worcester, the process to unblock is as follows:

* The teacher makes the request to the VW (Assistant Principal: Curriculum, Teaching & Learning). Or
* Care staff makes the request to KK (Head of Care)
* The e-safety coordinator or other nominated person checks the website content to ensure that it is appropriate for use in New College Worcester.
* If agreement is reached the e-safety coordinator requests the site be unblocked and logs the action in the change-control log to be reported as described above.

The e-safety coordinator will need to apply a rigorous policy for approving / rejecting filtering requests. This can be found in Appendix 3 but the core of this should be based on the site’s content:

* The site promotes equal and just representations of racial, gender, and religious issues.
* The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.

### B.2.1e Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The New College Worcester will therefore monitor the activities of users on the network and on New College Worcester equipment.

Monitoring takes place as follows:

* Identified members of staff (designated SLT member(s) / e-safety co-ordinator & JF(Head of IT)) review the monitoring reports in turn, weekly.
* Potential issues are referred to an appropriate person depending on the nature of the capture.
* Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. ‘goddess’ is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

### B.2.1f Audit /Reporting

Filter change-control logs and incident logs are made available to:

* the e-safety governor within the timeframe stated in section A.1.3 of this policy
* the e-safety committee (see A.1.1)
* the Worcestershire Safeguarding Children Board on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.

For example, the evidence might show a large number of requests to remove the filtering from sites – in which case NCW might question whether their current level of filtering is too restrictive for educational purposes. Alternatively, a large number of incidents where users try to subvert the filtering system might suggest that improved monitoring / disciplinary action might be necessary.

**Section C. Education**

**C.1.1 E-Safety Education**

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in E-Safety is therefore an essential part of NCW’s E-Safety provision. Children and young people need constant help and support to recognise and avoid E-Safety risks and build their resilience. This is particularly important for helping them to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

* A planned E-Safety programme is provided as part of IT, PSHCE and other lessons. This is regularly revisited, covering the use of IT and new technologies both at NCW and beyond.
* Key E-Safety messages will be reinforced through further input via assemblies and Form Group activities, as well as informal conversations when the opportunity arises.
* Students will be helped to understand the need for the pupil Acceptable Use Agreement (see Appendix 1) and encouraged to adopt safe and responsible use of IT both within and outside NCW.

In lessons where internet use is pre-planned, it is best practice that younger students should be guided to sites checked as suitable for their use. Processes should be in place, and known to students, for dealing with any unsuitable material that is found in internet searches.

Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging students to discuss anything of which they are unsure and implementing the NCW behaviour policy where appropriate.

Students will be made aware of what to do should they experience anything, while on the Internet, which makes them feel uncomfortable.

**C.1.2 Information Literacy**

Students will be taught in lessons to be critically aware of the content they access online and be guided to validate the accuracy of information by employing techniques such as:

* Checking the likely validity of the URL (web address).
* Cross checking references (Can they find the same information on other sites?).
* Checking the pedigree of the compilers / owners of the website.
* Referring to other (including non-digital) sources.

Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Students are taught how to make best use of internet search engines to arrive at the information they require

**C.1.3 The Contribution of the Students to the E-Learning Strategy**

Students are represented on the E-Safety Group. Two senior students will be identified by the E-Safety Co-ordinator and Vice Principal to attend meetings.

Students often use technology out of NCW in ways that are not usually found in the classroom. Members of staff are always keen to hear of their experiences and how they feel the technology (especially rapidly developing technology such as mobile devices) could be helpful in their learning.

Students play a part in monitoring this policy (see section A.1.1).

**C.2 Training**

All staff will be trained with respect to this policy. There will be regular update training in terms of key aspects of this policy.

Governors will all be aware of the policy and have opportunity to discuss its implications with members of the Senior Leadership Team. There will be regular communication between the NCW E-Safety Co-ordinator and the Governor with Responsibility for E-Safety. The E-Safety Co-ordinator will meet with the Governor with Responsibility for Safeguarding termly.

All parents will be alerted to this policy and will be able to access it on the NCW website. Parents will also have access to the DfE updates on E-Safety on the NCW website.

**Section D**

**Appendix 1**

**Acceptable Use Agreements**

# **ACCEPTABLE USE OF IT AND ELECTRONIC EQUIPMENT ON CAMPUS AND E-SAFETY POLICY**

### Introduction

New College Worcester (NCW) is required to run a safe and secure computer network, with licensed software and have a responsibility to train staff and students to use all aspects of IT safely and responsibly. Users of NCW IT systems must take responsibility for their actions, so reading, understanding and signing the Acceptable Use Agreement is an essential requirement. Breaching the terms of this agreement may lead to a disciplinary process which could result in College sanctions (including temporary or permanent exclusion) or dismissal, and prosecution. With regard to electronic equipment, NCW has further developed this Policy for students and staff on campus in response to the continuing increase in the use of personal mobile communication, social media and gaming technology.

### **USE OF IT EQUIPMENT ON CAMPUS**

### Facilities Offered

* NCW computer facilities are primarily for work and study
* Use for leisure and recreation is a privilege.
* An approved user accesses the network via an account provided, with a unique login name and a password.
* The range of services provided includes storage space for essential data on an automatically backed-up home drive; filtered Internet access; monitored e-mail; printing; embossing; Access Technology Software; Microsoft Office applications; desktop PCs; laptop computers; Braille Notes or any similar equipment or provision.

### Technical Support

* The College will assess need and provide appropriate IT equipment to enable students to learn effectively and to enable staff to perform their roles effectively.
* Technical support is only available for College IT resources; it does not extend to individuals and their personal property.

### The Law

* NCW users are subject to UK law, which covers copyright, misuse, data protection, defamation, and all forms of harassment, irrespective of the legality of the material in the country of its origin.
* Nothing should ever be written down that the author would not wish to have read out in open court.
* Hacking is “the unauthorised use, or attempt to circumvent or bypass the security mechanisms, of an information system or network” and is an illegal activity.

### Internet Filtering

* Users must not access inappropriate content, illegal software sites or anonymous proxy servers.
* Accidental visits to (or the discovery of) any such sites must be reported to a student’s teacher or form tutor, or an employee’s line manager and this information passed to the Network Manager.
* NCW cannot control the information from the Internet and therefore reserves the right to decide which sites are blocked. If a member of staff wishes to have a site unblocked to use with students or to enable them to perform their job effectively, they should pass the web address to the Vice Principal for checking.

**E-Mails**

* E-mail content must comply with NCW policies.
* The e-mail system is primarily for staff/students in relation to their work/studies.
* Limited personal use of the system is allowed but this must not impact adversely on work/studies and should be in staff/students leisure time.
* Any e-mails of a personal nature that are sent must not include NCW’s corporate signature.
* Staff e-mailing students should **always** do so through their college e-mail address and **not** through a personal e-mail address.

### Monitoring

* NCW monitors the use of Internet and e-mail services, and may, with good reason, examine the contents of certain e-mails, particularly if there are issues relating to safeguarding/radicalisation.

### Health and Safety

* IT users must pay regard to workstation comfort and posture, using appropriate accessories where required, taking regular breaks to avoid fatigue. Further guidance is available in the NCW Display Screen Use Policy (No 98).
* Attention must be paid to hazards, including trailing cables, electrical installations, lighting glare or reflections. (See NCW Health and Safety Policy (No 42)).

### E-Safety

* NCW must ensure the safety and wellbeing of all children and young people at the College and will ensure that IT systems and their use align with this imperative.
* Appropriate Internet filtering must be in place and monitored for any repeat or concerning behaviour by users of the IT network.
* IT filtering will ensure that any attempts by staff or students to access extremist websites will be blocked and reported.
* Students and staff will receive regular training and updates on e-safety issues through assemblies, PSHE, tutor times and staff training.
* Parents will receive information regarding e-safety as part of the regular communication from the College
* The e-safety committee will meet half-termly to develop policy, monitor incidents and students/staff concerns, and develop training.
* e-safety will be monitored through Governor committee and a link e-safety Governor
* a log of e-safety incidents will be kept by the Vice Principal and patterns and emerging trends assessed.

### Instant Messaging Services

* These are privileges reserved for leisure time, therefore restrictions and timings will apply.
* Students will be made aware of the danger of making contact with strangers online, and should ask for help or report any concerns to a responsible adult.

### Social Networking

* **Staff members must not be or become “friends” with current students on any social networking site, nor with former students until at least 2 years after they have left.**

Viruses and Malicious Code

* Restrictions and monitoring will be applied to downloading and uploading.
* Virus infections must be reported immediately.
* Any knowledge of hacking (as defined in the Section entitled “The Law”) must also be reported immediately.

### Confidentiality and Security

* All College IT equipment must be treated with due care and protected from accidental or deliberate damage.
* No IT systems are 100% secure.
* Users must not divulge their password to anyone.
* To prevent others from gaining unauthorised access to College information, computers or devices accessing College information must not be left logged on whilst unattended.
* When unattended, laptops and computers must be logged out or locked which can be done by pressing the window symbol key and L concurrently.
* NCW IT users who purchase goods or services for personal use online do so at their own risk.
* The security of all sensitive data stored in portable computer equipment must be managed with reasonable care and in accordance with NCW’s Data Protection Policy (No 46).
* For security and insurance purposes, College laptops should not be left in view in a car, left in the boot of a car for an extended time or left unattended in a public place.

**Return of Equipment**

* Both staff and students must be aware that IT equipment provided by the College is on loan to them during their time at the College.
* It is the responsibility of the member of staff or the student to ensure that laptops etc are returned to the College before they leave. User login accounts, which allow access to the College network and email system, are disabled when a member of staff or student leaves the College. If a student requires any of their work for future reference, they should save this to another device before returning their laptop.
* If equipment is not returned appropriately, the College reserves the right to invoice the member of staff or student for the replacement cost.

**USE OF ELECTRONIC EQUIPMENT ON CAMPUS**

All staff and students are allowed to use their personal devices. Examples of these devices are mobile phones, laptop computers and more relevant to students games consoles e.g. play station.

The aim of the policy is:

* To make staff aware of the implications of using their own equipment on campus.
* To allow students to take advantage of the convenience, privacy, usefulness and pleasure that these devices offer.
* To make staff, students, parents and guardians aware of what controls NCW will impose on the use of personal devices by students on campus.

The College will not be responsible for:

* Any loss of, theft of, or damage to a device.
* The costs involved whilst using a device e.g. mobile phone.

The College will monitor the extent to which a student uses his/ her device/s particularly when it is:

* Having a detrimental effect on a student’s academic work, and/or social interaction
* Being used inappropriately and at inappropriate times and places

**General Rules:**

* Mobile phones must not be used in lessons without the teacher’s permission and only for educational use..
* They may be used by students in the Houses/Hostel and on other areas of the campus (except for the main building) between 4.00 pm and bedtime (unless restrictions have been applied due to misuse or in terms of student welfare).
* The devices should not be used in the Dining Room. They should be switched off or not taken in at all. The same applies to functions like College concerts, plays etc.
* Students should not connect their devices to any equipment that does not belong to them. Mobile phones should not be connected to College network computers and College laptop computers.
* All devices and associated battery chargers are required to be safe for use; they will need to pass the Portable Appliance Test (PAT).
* Any damage caused by a student’s use of a device or its battery charging equipment will be the responsibility of the student’s parent / guardian.

**House/Hostel Rules:**

Students:

* should not use laptops and gaming devices after their bedtime.
* are responsible for the security and upkeep of their devices.

should not use the devices to cause a nuisance or disturbance in the House/Hostel or on campus.

**The Law**

* Consideration is given to individual circumstances of children in watching videos and television, and in using computer games and accessing the internet.
* Videos, games consoles and other computer games may only be watched/played by children of the intended age range.
* The College shall not have any videos or games certified as only suitable for over 18’s in areas where they could be accessed by those under 18.
* Systems and policies are in place to safeguard children when computer networking or on the internet and also to prevent excessive use of the television and computers.

**Sanctions:**

* If a student is found not to be following the guidelines above when using a device, it will be confiscated temporarily.
* Students may have restrictions placed on the use of electronic equipment if they do not adhere to the requirements of this Policy or if it is judged to be in their best interests.
* Parents will be informed of the action.
* The College will not be liable for any charges incurred (e.g. line rental) during the period of confiscation.
* If a user of College IT equipment is found to have broken the law in using that equipment, the Police will be notified. This also applies to anyone using their own IT equipment on College premises or on the campus.

*(Signature slip will be attached to the policy – to be returned to Admin to put on staff/student file.*

**Appendix 1b Signature slip for E-Safety Policy**

****

**NEW COLLEGE WORCESTER.**

**E-SAFETY POLICY FOR NEW COLLEGE WORCESTER**

**(POLICY NUMBER 163).**

I have read and understood the information in the E-Safety Policy (Policy Number 163). I agree to abide by this policy. I understand that failure to comply may result in temporary or permanent suspension of my use of any part or all of the NCW IT systems and equipment and may incur financial penalties.

**I, ………………………………………………………………...**

**(BLOCK CAPITALS) hereby confirm that I have read and understood the document entitled:- E-Safety Policy (Policy Number 163)**

**SIGNED…………………………………………….…. DATE…………………**

For office use only:

**TO DATABASE AND STAFF/STUDENT FILE**

**D Appendix 2 E-Safety Curriculum**

E-safety curriculum

Autumn 1 privacy/security

Autumn 2 cyberbullying

Spring 1 relationships/communications

Spring 2 self-image and digital identity, online reputation and digital footprint

Summer 1 information literacy

Summer 2 creative credit/copyright

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| strand | privacy/security | cyberbullying | internet safety, relationships, communication | digital footprint reputation, self-image/identity  | information literacy | creative credit copyright |
| When | Autumn 1 | Autumn 2 | Spring 1 | spring 2 | Summer 2 | Summer 2 |
| Components | managing online information and keeping it secure from online risks, how to avoid scams and schemes and how to analyse privacy policies | What to do if they are involved in a cyberbullying situation. Explore the roles people play and how individual actions, both positive and negative, can impact their networks. Students are encouraged to be upstanders and to build positive and supportive online relationships | distinguishing between inappropriate contact and positive connections.Explore how the internet offers an amazing way to collaborate with others worldwideReflect on how intrapersonal and interpersonal skills to build and strengthen positive online communication and communities. | considering how what is shared online can impact self and others.helping students explore their own digital lives. The benefits and risks of personas and the effect on their sense of self, their reputation and their relationships | Finding, identifying, evaluating and using information effectively. | responsibilities and rights as creators in the online spaces in which consumption, creation and sharing of information takes place |
| Year 7 | secure password **(ICT)** | Be upstanding – students learn the difference between being a passive bystander and a brave upstander **(FT/HOKS)****Resist online peer pressure** | know how to report concerns and inappropriate behaviour **(FT/HOKS)****resist online peer pressure**Students are introduced to the 24/7 social nature of digital media and technologies, and gain basic vocabulary and knowledge for discussing the media landscape **(FT/HOKS/ICT)** | ‘think before you act’ online **(FT/HOKS/ICT)** | strategic searching – learning how to use keywords on the internet **(HUMANITIES)** |  |
| Year 8 |  | safe social networking – reporting abuse **(FT/HOKS)** | desensitisation **(FT/HOKS)**safe social networking**(FT/HOKS/CARE)**safe online talk – while acknowledging the benefits of online talk and messaging, students learn how to handle situations or online behaviour that makes them feel uncomfortable **(FT/HOKS/CARE)** | permanency and possible duplication of what we post online **(IT)**social networking profile **(FT/HOKS)**Students review their media habits and reflect on the role of digital media in their lives.**(ENGLISH)**Which me should I be – presenting yourself in different ways online carries both benefits and risks **(FT/HOKS)** |  | Students reflect on their responsibilities as creators and users of creative work **(art, drama, music)** |
| Year 9 |  | crossing the line – learning how to make the distinction between good-natured teasing and bullying **(FT/HOKS)****resist online peer pressure** | how to recognise grooming **(FT/HOKS/CARE)** | online reputation trillion dollar footprint **(IT)** | how to identify high-quality sites **(SCIENCE)** | plagiarism **(ART, DRAMA, MUSIC)** |
| strand | privacy/security | cyberbullying | internet safety relationships, communication | digital footprint reputation self-image/identity | information literacy | creative credit copyright |
| Year 10 |  | turn down the dial – learning that cruelty can escalate quickly online – anonymity and lack of responsibility **(FT/HOKS)** | Gender stereotyping – dress up your avatar – virtual world for kids for evidence of stereotypes about boys and girls. **(PSHCE)** | oops I put it online – introduction to the benefits of sharing online and the risks of sharing inappropriate information.Digital life – the role digital media plays in your life **(PSHCE)** | PSHCE unit on information retrieval | concept of creative commons **(?)** |
| Year 11 | exploring the concept of privacy in their everyday lives and as it relates to using the internet **(PSHCE)** |  | thinking critically about developing relationships online my online code – ethical behaviour online.Romantic relationships online – risks and responsibilities **(PSHCE)** | who are you online – how people represent themselves online and the relationship between online and offline selves **(PSHCE)** | building online communities – websites that foster positive community **(PSHCE)** |  |
| strand | privacy/security | cyberbullying | internet safety relationships, communication | digital footprint reputation self-image/identity | information literacy | creative credit copyright |
| Year 12 |  | perspectives on cyberbullying – the dynamics of online cruelty and how it affects all the people involved **(FT/HOKS)** |  | college bound – everything they or anyone else posts about them becomes part of a public online presence known as a digital footprint **(FT/HOKS)** |  | learning the difference between getting inspiration from the creative work of others, and appropriating that work without permission. **(ENHANCEMENT)** |
| Year 13, 13+ | Does it matter who has your data? Considering the ways in which websites and companies collect data online and personalise it for their users, and considering companies’ motives for doing so **(FT/HOKS)** | learning the definition of hate speech and understand how it affects individuals, groups and communities **(ENHANCEMENT)** | reflecting on the responsibility to protect the privacy of others when posting information about them online **(FT/HOKS)** |  | considering the benefits and drawbacks of using collective intelligence in different contexts **(FT/HOKS)** |  |

**D Appendix 3 Supporting Resources and Links**

The following links may be helpful:

**General**

* **South West Grid for Learning** “SWGfL Safe” - http://www.swgfl.org.uk/Staying-Safe
* **Child Exploitation and Online Protection Centre (CEOP)**  <http://www.ceop.gov.uk/>
* **ThinkUKnow** <http://www.thinkuknow.co.uk/>
* **ChildNet** <http://www.childnet-int.org/>
* **InSafe** <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>
* **Byron Reviews** (“Safer Children in a Digital World”) - http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews
* **Becta –** various useful resources now archived [http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk](http://webarchive.nationalarchives.gov.uk/20101102103654/http%3A/www.becta.org.uk)
* **National Education Network** NEN E-Safety Audit Tool - [http://www.nen.gov.uk/hot\_topic/13/nen-E-Safety-audit-tool.html](http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html)
* **WMNet** – http://[www.wmnet.org.uk](http://www.wmnet.org.uk)
* **EU kids Online** - [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx](http://www2.lse.ac.uk/media%40lse/research/EUKidsOnline/Home.aspx)

**Cyber Bullying**

* **Teachernet “Safe to Learn – embedding anti-bullying work in Colleges”** (Archived resources)

[http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeCollege/behaviour/tacklingbullying/cyberbullying/](http://tna.europarchive.org/20080108001302/http%3A//www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/)

* **Anti-Bullying Network** - <http://www.antibullying.net/cyberbullying1.htm>
* **Cyberbullying.org** - <http://www.cyberbullying.org/>
* **East Sussex Council** - Cyberbullying - A Guide for Colleges:

52

<https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx>

* **CyberMentors:** young people helping and supporting each other online - <http://www.cybermentors.org.uk/>

**Social Networking**

* **Digizen** – “Young People and Social Networking Services”: <http://www.digizen.org.uk/socialnetworking/>
* **Ofcom Report**: Engaging with Social Networking sites (Executive Summary)

[**http://www.ofcom.org.uk/advice/media\_literacy/medlitpub/medlitpubrss/socialnetworking/summary/**](http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/)

* **Connect Safely -** Smart socialising: <http://www.blogsafety.com>

**Mobile Technologies**

* **“How mobile phones help learning in secondary schools”:**

<http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf>

* **“Guidelines on misuse of camera and video phones in Colleges**” <http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf>

**Data protection and information handling**

* **Information Commissioners Office** - Data Protection:

<http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx>

See also Becta (archived) resources above

* **Parents’ guide to new technologies and social networking**

<http://www.iab.ie/>

<http://www.vodaphone.com/parents>

**Links to Other Resource Providers**

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and College staff. A comprehensive list of these resources (and those available from other organisations) is available on:

* “SWGfL Safe” website: <http://www.swgfl.org.uk/staying-safe>
* BBC Webwise: <http://www.bbc.co.uk/webwise/>
* Kidsmart: <http://www.kidsmart.org.uk/default.aspx>
* Know It All - <http://www.childnet-int.org/kia/>
* Cybersmart - <http://www.cybersmartcurriculum.org/home/>
* NCH - <http://www.stoptextbully.com/>
* Chatdanger - <http://www.chatdanger.com/>
* Internet Watch Foundation: <http://www.iwf.org.uk/media/literature.htm>
* Digizen – cyber-bullying films: <http://www.digizen.org/cyberbullying/film.aspx>
* London Grid for Learning: <http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel>

**Appendix 4 - Glossary of Terms**

* AUA Acceptable Use Agreement – see templates earlier in this document.
* Becta: British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
* CEOP: Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
* DfE: Department for Education
* FOSI: Family Online Safety Institute
* ICT: Information and Communications Technology
* ICT Mark: Quality standard for school/academies provided by NAACE for DfE
* INSET: In-service Education and Training
* IP address: The label that identifies each computer to other computers using the IP (internet protocol)
* ISP: Internet Service Provider
* IWF: Internet Watch Foundation
* JANET: Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
* KS1; KS2 KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 2 to 6 (age 7 to 11)
* LA Local Authority
* LAN Local Area Network
* Learning platform (An online system designed to support teaching and learning in an educational setting)
* LSCB Local Safeguarding Children Board
* MIS Management Information System
* NEN National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to Colleges across Britain.
* Ofcom Office of Communications (Independent communications sector regulator)
* Ofsted Office for Standards in Education, Children’s Services and Skills
* PDA Personal Digital Assistant (handheld device)
* PHSE Personal, Health and Social Education
* SRF Self Review Framework – a tool maintained by Naace used by Colleges to evaluate the quality of their ICT provision and judge their readiness for submission for the ICT Mark
* SWGfL South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to E-Safety (on whose policy this one is based)
* URL Universal Resource Locator – a web address
* WMNet The Regional Broadband Consortium of West Midland Local Authorities – provides support for all Colleges in the region and connects them all to the National Education Network (Internet)
* WSCB Worcestershire Safeguarding Children Board (the local safeguarding board)

 163 E-Safety Policy

Initially adopted: Jan 2017

Equality and Diversity Check: Sarah Smith Jan 2017

Reviewed: June 2018

Next review due: June 2019

Person responsible for review: Assistant Principal (Business and Finance)/E-Safety Co-ordinator

Date Approved by SLT: 26/06/17

26/11/18

Out for consultation:

Date Approved by RC& SC: 07/11/17

14/11/18

Date approved by Governors: 19/07/17

Date Issued to Staff: On Staff Drive 13/11/17

27/11/18

Date Issued to Students:

Date Issued to Parents:

On Staff Drive: 13/11/17

19/11/18

Sent in Starter Pack

Included in Induction Pack

On website