WORCESTER
SIXTH FORM COLLEGE

ONLINE SAFETY POLICY AND PROCEDURES

Sept 2024

ONLINE SAFETY POLICY AND PROCEDURES

Responsibility

SLT member: Designated Senior Lead for Safeguarding
Working with: All staff and students

Aim

One of the main applications of technology that people use today is the internet. Worcester Sixth Form College acknowledges that staying safe online is an increasingly complex issue and are committed to educating and supporting students and staff in online safety matters.

Policy Scope

This policy applies to all students and staff within the College community who have access to the College IT systems, both on the premises and remotely and applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites and mobile devices.

Any user of College IT systems is required to agree to adhere to the Acceptable Use Policy (AUP) alongside this policy

Policy Statement

Worcester Sixth Form College recognises the benefits and opportunities which internet technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. Our approach is to implement appropriate safeguards within the College while supporting users to identify and manage risks independently and with confidence.

Users will have access to the Internet and email on all networked computers and mobile device technology used in the College for research and education purposes. WSFC welcomes this as a means of improving the IT skills of users and as an aid to teaching and learning. Additionally, students and staff may also connect to the College wireless network on their mobile devices in order to access the internet.

Students will receive an induction to IT Services provided at the College during one of their initial group tutorial sessions. Similarly, new staff are given login details and undergo continual training to use the college systems. Both groups must agree to abide by the Acceptable Use Policy and this Online Safety Policy as part of their induction process

All students will be educated on online safety through sessions which they all undertake as part of their Tutorial programme in their first year of study.

Roles and Responsibilities

There are clear lines of responsibility for online safety within the College.

All students must know what to do if they have online safety concerns and who to talk to (see Appendix 1 for details of key personnel who have specific e-safety responsibilities at WSFC). In most cases, incidences and concerns which are raised by students with regards to their online safety (e.g. bullying/harassment, grooming) will be dealt with by the allocated Head of Year or in their absence the designated person with responsibility for safeguarding. Where any report of an online safety incident is made, all parties should know what procedure is triggered and how this will be followed up. This will be discussed with the student/person reporting the incident. Incidents involving staff will be dealt with by the Principal and Designated Safeguarding Lead.

Where management considers it appropriate, the designated persons may be asked to intervene with appropriate additional support from external agencies including the Police.

- All users are responsible for using the College IT systems and mobile devices in accordance with the *Acceptable Use Policy* which they must sign at the time of registration or induction.
- All users must act safely and responsibly at all times when using the internet and/or mobile technologies.
- Students are responsible for attending online safety lessons as part of their Tutorial programme and are expected to know and act in line with other relevant College policies with regards to online safety matters and in particular mobile phone use, sharing images, cyber-bullying etc. Staff are made aware of expectations during induction procedures.
- Students must follow reporting procedures where they are worried or concerned, or where they believe an online safety incident has taken place involving them or another member of the College community. Further guidance is available in the flow chart in Appendix 1.

Filtering and monitoring

As stated in the Acceptable Use Policy the College has a statutory duty to carry out appropriate filtering and monitoring to keep students safe and free from harm. The college recognises its responsibilities set out in Keeping Children Safe in Education (2024) which requires us to identify potential risk in the ICT environment, intervening and escalating any concerns raised as necessary.

The guidance identifies four categories of online risk that staff and students should be aware of, and the college internet filter and monitoring procedures are set up to protect users that may try to access websites within the scope of these categories:

1. **content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
2. **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
3. **conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
4. **commerce**: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

The College has effective filtering (e.g. the college firewall) and monitoring software (e.g. Smoothwall) which is operational on college devices and across the Wired and Wi-Fi network so that we can fulfil these requirements and support and intervene when any safeguarding reports are initiated through the software. The software monitors use of College devices and identifies any safeguarding concerns and issues (cyberbullying, radicalisation, abuse) which may result in reports being made and send to the Designated Safeguarding Lead and Deputy Safeguarding Leads for consideration so that any incidences can be acted upon swiftly and escalated and reported as appropriate. Reports of any safeguarding, child protection concerns are produced in real time so that any concerns identified can be dealt with immediately with users.

The filtering and monitoring software providers college use are members of the Internet Watch Foundation. They use rules for traffic and therefore can block traffic on both BYOD and college devices. It does block multi-lingual web content, misspellings and abbreviations. Additionally, 'Safe search' is applied to all of our internet searches through the internet filter. The blocked list is provided by our filtering company who is a major education provider and reviewed yearly with the DSL. Filter logs are reviewed regularly by the Senior Lead for ILT strategy and ongoing updates are applied to the blocked list alongside adhoc site blocking requests from teaching staff.

All of these systems are put through the South West Grid for Learning (SWGfL) testing tool regularly http://testfiltering.com

Security

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date and appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc. to prevent accidental or malicious access of College systems and information or bypassing of these systems.

All users should use strong passwords for any IT accounts including their college password. These are long (at least 15 characters) and have a combination of upper and lower case letters, numbers and one or more special keyboard characters such as the asterisk or currency symbols.

Behaviour

Worcester Sixth Form College will ensure that all users of technologies adhere to the standard of behaviour as set out in the *Acceptable Use Policy* and this policy.

The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the *Anti-Bullying and Harassment Policy and Procedures* and *Acceptable Use Policy.*

Where conduct is found to be unacceptable, the College will deal with the matter internally using the appropriate conduct policy. Where conduct is considered illegal, the College will seek advice, support and guidance appropriately, report the matter to the police and any other relevant external agencies.

Social Media

Social Media sites are powerful tools that, if used in the correct 'safe' way, can be a great way to socialise, broadcast, share, voice opinions, and network. However, they can also be very dangerous if used incorrectly ruining relationships and potentially affecting future career and university options. Several departments in college recommend Social Media sites which are used to support teaching and learning in those curriculum areas.

The following is a set of guidelines to help users safely enjoy social media:

Do

- Regularly check and change your privacy settings.
- Be Respectful to others online, to others and yourself.
- Use a strong password and change it regularly.
- Read the privacy policy of the site.
- Check the privacy policy and authenticity of apps that you may add.
- Remember what you post can affect you in the real world, universities and future employers may check your social media profiles.
- ALWAYS report cyber bullying to a parent/guardian/tutor/teacher/line manager.

Don't

- Let your friends pressure you into doing something on social media sites that you are not comfortable with.
- Leave your profile logged in, if you are using your smart phone to access social media, password protect your phone.
- Never click on links or install applications that are sent to you if you're not expecting them.

Use of Images and Video

The use of images, or photographs, is popular in learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

All students will receive training in their online safety session incorporated into the Tutorial programme which considers the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

The College requires all students to check and comply with copyright laws when using any images within their classwork, homework, coursework or other College activity. This includes images downloaded from the internet and images belonging to staff or students.

Personal Information

Personal information is information about a particular living person. Worcester Sixth Form College collects and stores the personal information of students regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The College will keep that information safe and secure and will not pass it onto anyone else without the permission of the student.

No personal information will be posted to the College website or social media without the permission of the student. Only names and work email addresses of (senior) staff will appear on the College website and no students' personal information will be available on the website without permission.

Staff will keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.

All College mobile devices such as a laptop, USB (containing personal data) are required to be encrypted, password protected and signed out by a member of the IT staff before leaving the premises.

Where the personal data is no longer required, it must be securely deleted in line with the College *Data Protection Policy & Procedures.*

Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for students. It is our view therefore, that the College should support students to stay safe online through regular training and education. This will provide students with skills to be able to identify risks independently and manage them effectively. Any training in relation to online safety is compulsory.

Students will attend online safety sessions within the Tutorial programme which is compulsory for all students within College. The first of these will take place during the first half term at the beginning of the College year.

Issues associated with online safety apply across the curriculum and students should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies within their academic areas.

Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. A link to the College online safety policy is accessible for students, parents and staff use and key safety messages are highlighted in posters and leaflets around College.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Incidents and Response

Where an online safety incident is reported to the College this matter will be dealt with very seriously.

The College will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can do so to their Tutor, Head of Year or the Network Manager/Network Administrator according to the Incident report flow chart in Appendix 2.

Following any incident, the College will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Related Policies and Procedures

This online safety policy should be read alongside other relevant College policies:

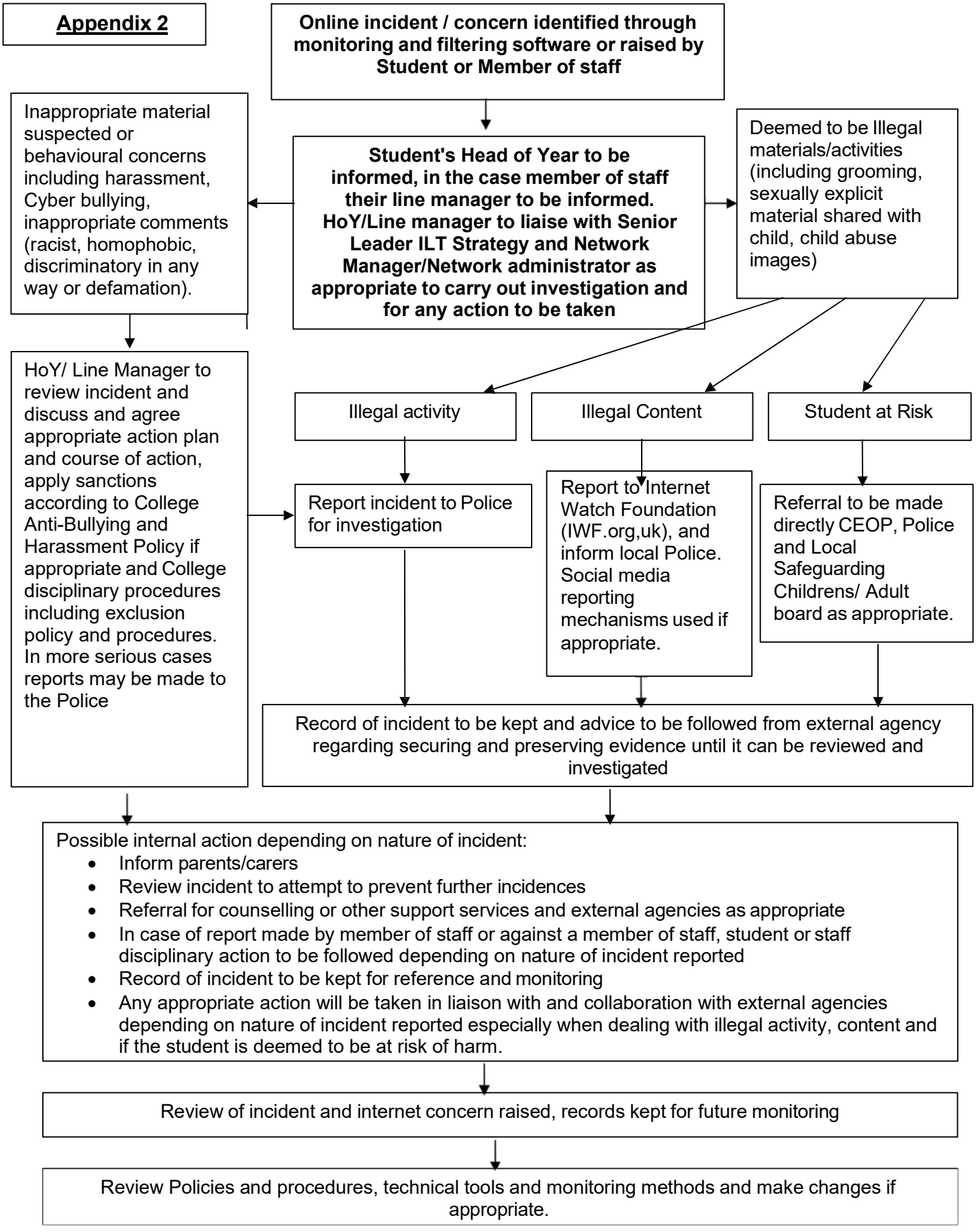
- *Safeguarding and child protection Policy and Procedures*
- *Anti-Bullying and Harassment Policy and Procedures*
- *Acceptable Use Policy*
- *Data Protection Policy and Procedure*

Appendix 1

Key roles and responsibilities for online safety at Worcester Sixth Form College

Graham Williams	Designated Senior Lead for Safeguarding graham.williams@wsfc.ac.uk Ext: 612
Heather Anderson-Stevens	Deputy Designated Safeguarding Lead heather.anderson-stevens@wsfc.ac.uk Ext: 614
Claudia Cole	MIS Manager & Data Protection Officer claudia.cole@wsfc.ac.uk Ext: 610
Carl Rusby	Senior Leader (ILT Strategy) carl.rusby@wsfc.ac.uk Ext: 633
Mark Leaney	Network Manager mark.leaney@wsfc.ac.uk Ext: 1001

Appendix 2


Online incident / concern identified through monitoring and filtering software or raised by Student or Member of staff
Inappropriate material suspected or behavioural concerns including harassment, Cyber bullying, inappropriate comments (racist, homophobic, discriminatory in any way or defamation).
Student's Head of Year to be informed, in the case member of staff their line manager to be informed. HoY/Line manager to liaise with Senior Leader ILT Strategy and Network Manager/Network administrator as appropriate to carry out investigation and for any action to be taken
Deemed to be Illegal materials/activities (including grooming, sexually explicit material shared with child, child abuse images)
HoY/ Line Manager to review incident and discuss and agree appropriate action plan and course of action, apply sanctions according to College Anti-Bullying and Harassment Policy if appropriate and College disciplinary procedures including exclusion policy and procedures. In more serious cases reports may be made to the Police
Illegal activity
Illegal Content
Student at Risk
Report incident to Police for investigation
Report to Internet Watch Foundation (IWF.org,uk), and inform local Police. Social media reporting mechanisms used if appropriate.
Referral to be made directly CEOP, Police and Local Safeguarding Childrens/ Adult board as appropriate.
Record of incident to be kept and advice to be followed from external agency regarding securing and preserving evidence until it can be reviewed and investigated
Possible internal action depending on nature of incident:
• Inform parents/carers
• Review incident to attempt to prevent further incidences
• Referral for counselling or other support services and external agencies as appropriate
• In case of report made by member of staff or against a member of staff, student or staff disciplinary action to be followed depending on nature of incident reported
• Record of incident to be kept for reference and monitoring
• Any appropriate action will be taken in liaison with and collaboration with external agencies depending on nature of incident reported especially when dealing with illegal activity, content and if the student is deemed to be at risk of harm.
Review of incident and internet concern raised, records kept for future monitoring
Review Policies and procedures, technical tools and monitoring methods and make changes if appropriate.