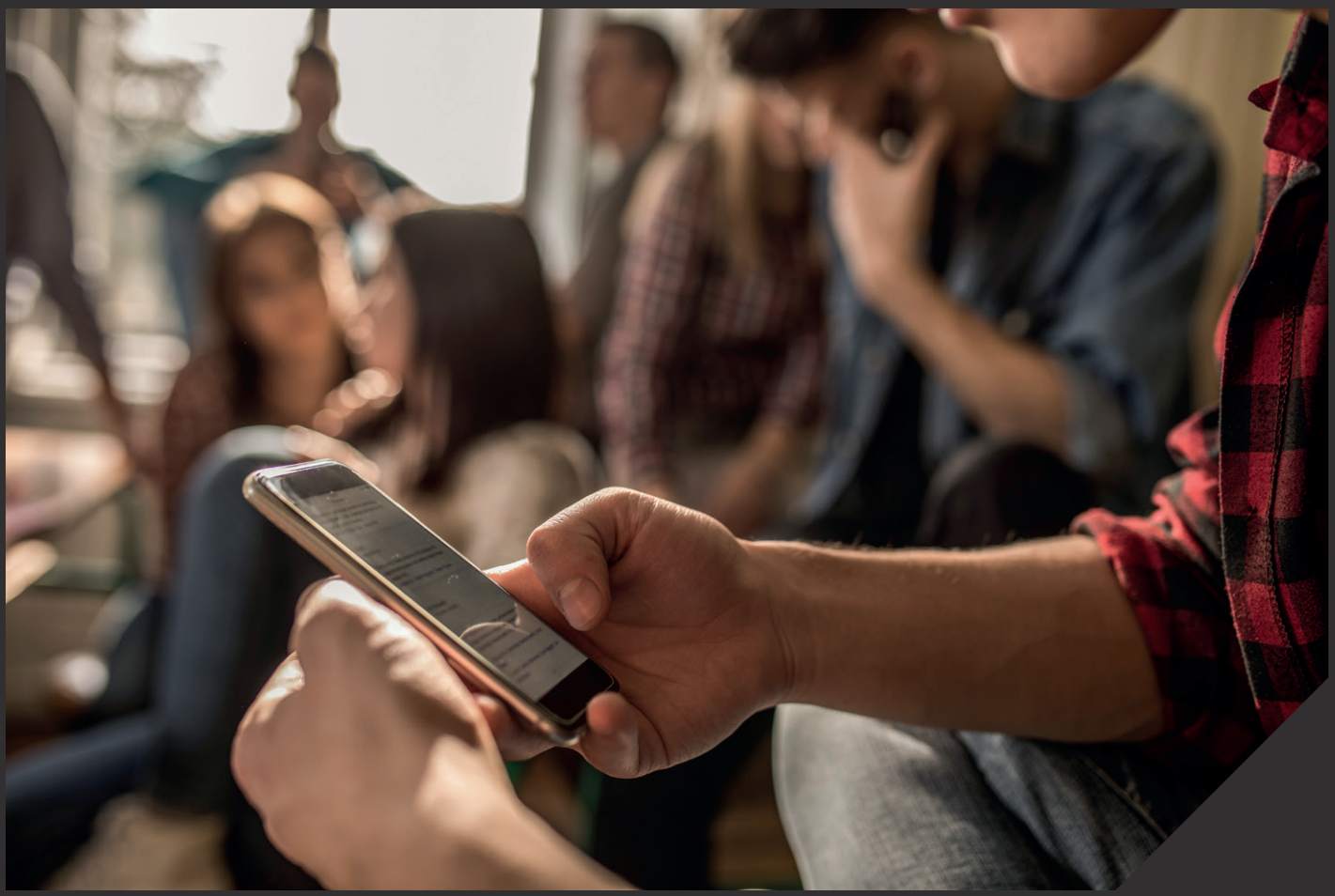
University of Suffolk

Office for Students

HIGHER EDUCATION ONLINE SAFEGUARDING SELF-REVIEW TOOL

2019

By Professor Emma Bond and Professor Andy Phippen



Introduction

While student safeguarding is a well-established responsibility for UK higher education institutions, good practice in online safeguarding is only recently becoming recognised across the sector. The launch of the Universities UK 'Changing the Culture' report (UUK, 2016)[1] examining university students' experiences of violence against women, hate crime and harassment called for further action to specifically tackle online harassment and hate crime. Online harms are well acknowledged in the compulsory educational sector and exemplified by the Ofsted inspection framework (2018)[2] and the Department for Education's (DfE) (2018)[3] Keeping children safe in education: Statutory guidance for schools and colleges. Such harms do not necessarily cease when young people enter into late adolescence and early adulthood.

However, in spite of a duty of care accorded to UK universities to act reasonably in students' best interests, to protect their well-being and to provide support as they continue in education (UUK, 2017)[4], there remains a lack of guidance in relation to current practice and regulation around online safety within higher education.

In response, a tool – developed by the University of Suffolk as part of the Office for Students Catalyst funded programme to support good practice in safeguarding students – focuses on tackling sexual violence, hate crime and online harassment, and is designed for higher education institutions to self-review their online safeguarding practice.

1 UUK (2016) Changing the Culture: Report of the Universities UK Taskforce examining violence against women, harassment and hate crime affecting university students available from https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2016/changing-the-culture.pdf

2 Ofsted (2018) School inspection handbook Handbook for inspecting schools in England under section 5 of the Education Act 2005 available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730127/School_inspection_handbook_section_5_270718.pdf

3 DfE (2018) Keeping children safe in education Statutory guidance for schools and colleges available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/741314/Keeping_Children_Safe_in_Education__3_September_2018_14.09.18.pdf

4 UUK (2017) Changing the culture: One year on – an assessment of strategies to tackle sexual misconduct. Available from https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2018/changing-the-culture-one-year-on.pdf

This tool defines 23 features of related policy and practice around online safeguarding for higher education institutions. Each feature can be self-assessed at four levels, graded from 0 to 3.

The levels are defined as:

Level	Definition
Level 0 – Reactive	There is no policy or practice in place, and issues are dealt with only reactively.
Level 1 – Basic	There is a simple definition of policy or fundamental aspects of practice, but they are not detailed in scope/ scale, or embedded in routine practice.
Level 2 – Embedded	Policy and practice are embedded and students are included in their development. Policies are detailed and proactive. Practice is applied across the institution in all departments and faculties.
Level 3 - Holistic	There is a sound understanding of how policy and practice work together to safeguard students online. There is ongoing reflection of best practice, and knowledge is shared across the institution and with statutory and non-statutory organisations in the community.

How to use the tool:

The tool provides clear definitions for 23 features and levels related to online safeguarding. For each feature a level can be determined by reading the level descriptions and deciding which one fits your own institutional practice most closely. Or, for a feature where institutional practice does not meet the definition for level 1, you can score that feature as level 0. Once you have defined baseline policy and practice at your institution you can use the tool to inform the development of an improvement plan, which can be regularly reviewed as policy and practice improves. The definitions for higher levels in each feature give clear guidance on how to enhance online safeguarding practice. The tool and improvement plan can be updated as policy and practice in your institution develops.

These features are clustered into four groups related to key aspects of safeguarding:

Policy	Education and training	Technology	Practice
The guiding principles related to an aspect of safeguarding that provide the foundation for practice in the institution.	How technological tools are used to help deliver policy and practice related to online safeguarding, is developed in the institution for both staff and students.	How technological tools are used to help deliver policy and practice related to online safeguarding.	How policy is implemented across the institution to deliver an institutional culture around online safeguarding.

Feature Definitions

Level 1 – Basic	The institution has basic policies and practices in place to respond to incidents as they occur. They strive to respond effectively in a timely and appropriate manner.
Level 2 – Embedded	The institution has policies and established practices in place that are embedded across the organisation. This allows it to be pro-active and pre-emptive to online safeguarding incidents, as well as responding appropriately and effectively.
Level 3 - Holistic	The institution has a well-established and clearly communicated culture across the organisation. Policies and practices are progressive and pro-active, and deal with online safeguarding incidents pre-emptively. The policies and practices of incident response consider broader aspects of prevention, such as well-being and resilience.

1. Policy related features **The list below is not prescriptive; some institutions will have policies that address the features below but use different names. The example terminology is advisory only, and there are many other policies into which these features fit or can be combined (for example anti-bullying might be a stand-alone policy, and may contain specific reference to image-based abuse).**		**Our level**
a. Anti-bullying/ harassment Institutional anti-bullying/harassment policies should also consider online elements to bullying and harassment, how they are tackled and how sanctions are brought into play.	**Level 1 — Basic** A basic policy is in place to meet the requirements of bullying and harassment. It includes definitions of bullying and harassment, and how digital technology can play a role in these. It should also specify how the university will respond to bullying and harassment concerns.	
	Level 2 — Embedded A detailed policy is in place to address bullying and harassment issues. It includes definitions of bullying, harassment and image-based abuse, and how digital technology can play a role in these. It should also specify how the university will respond to bullying and harassment concerns. The anti-bullying policy refers to other policies, such as student and staff code of conduct/acceptable use, safeguarding, dignity at work/study policies and disciplinary procedures. Stakeholders are aware of the policy and how it can be applied.	
	Level 3 — Holistic A detailed policy is in place to address of bullying and harassment issues. It includes definitions of bullying and harassment, and how digital technology can play a role in these. It should also specify how the university would respond to bullying and harassment concerns. The anti-bullying policy refers to other policies, such as student and staff code of conduct/acceptable use, safeguarding, dignity at work/study policies and disciplinary procedures. Stakeholders are aware of the policy and how it can be applied. The policy is informed from multi-stakeholder input, including external stakeholders. A multi-stakeholder committee regularly reviews the policy, using data collected by the university on bullying and harassment incidents. Policy relates to other aspects of university practice (such as student well-being) and engages readily with both internal (SU, chaplaincy, counselling) and external stakeholders (GPs, adult mental health services, police).	

1. Policy related features (continued)		Our level
b. Data protection How does the institution manage data on safeguarding issues relating to staff and students? How do they ensure data protection practices are compliant with legislation where there may be some conflict between data protection and safeguarding?	**Level 1 — Basic** Data protection policies include safeguarding concerns, and safeguarding practices have been audited to ensure data protection compliance.	
	Level 2 — Embedded Data protection policies include safeguarding concerns, and safeguarding practices have been audited to ensure data protection compliance. Those with responsibility for safeguarding are aware of –and have received training in – data protection practices in line with the statutory requirements of the institution.	
	Level 3 — Holistic Data protection policies include safeguarding concerns, and safeguarding practices have been audited to ensure data protection compliance. Those with responsibility for safeguarding are aware of, and have received training in data protection practices in line with the statutory requirements of the institution. Detailed data audits by the institution's Data Protection Officer are conducted regularly, and policy and practice are updated as a result.	
c. Equality and diversity policy Within this policy there may be elements related to hate crime with an online aspect that need to be considered. Specifically, consideration needs to be made around students with 'protected characteristics' – including age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race and ethnicity, religion or belief, and sexual orientation. Acknowledgement should be made in the policy to how protected characteristics may place students at great risk.	**Level 1 — Basic** The Equality and Diversity Policy considers online elements to hate crime and how the institution responds to them.	
	Level 2 — Embedded The Equality and Diversity Policy considers online elements to hate crime in detail and how the institution responds to them. The policy clearly relates online incidents to other policies (such as online safeguarding and anti-bullying) and differentiates those that might incorporate aspects of hate crime, stating why they should be tackled in order to incorporate equality and diversity into hate crime legislation. The policy considers escalating online hate incidents to other agencies (e.g. police).	
	Level 3 — Holistic The Equality and Diversity Policy considers online elements to hate crime in detail and how the institution responds to them. The policy has prevention strategies in place through raising awareness of local and national campaigns and education programmes. It clearly relates online incidents to other policies (such as online safeguarding and anti-bullying) and differentiates those that might incorporate aspects of hate crime, stating why they should be tackled in order to incorporate equality and diversity into hate crime legislation. The policy considers escalating online hate incidents to other agencies (e.g. police). The policy relates to other aspects of university practice, such as student well-being, and engages readily with both internal (SU, chaplaincy, counselling) and external stakeholders (GPs, adult mental health services, police).	

1. Policy related features (continued)		Our level
d. Governance structure This details the staff responsible for governance related to online safeguarding, which may include responsibility in the SLT, central teams, academic and professional support in faculties, students' union, external statutory partners (e.g. adult mental health, GPs, police, adult safeguarding), and non-statutory bodies (e.g. rape crisis, domestic abuse agencies, faith and race-based support organisations, Revenge Porn Helpline)	**Level 1 — Basic** There is a basic structure in place that identifies key roles in online safeguarding across the university, the staff members in those roles, and what is expected of them. Clear lines of communication are defined so staff know who to report online safeguarding matters to.	
	Level 2 — Embedded There is a basic structure in place that identifies key roles in online safeguarding across the university, the staff members in those roles, and what is expected of them. Clear lines of communication are defined so staff know who to report online safeguarding matters to. The structure should also include external stakeholders from both statutory (e.g. adult mental health, GPs, police, adult safeguarding) and non-statutory bodies (e.g. rape crisis, domestic abuse agencies, faith and race-based support organisations, Revenge Porn Helpline).	
	Level 3 — Holistic There is a basic structure in place that identifies key roles in online safeguarding across the university, the staff members in those roles, and what is expected of them. Clear lines of communication are defined so staff know who to report online safeguarding matters to. The structure should also include external stakeholders from both statutory (e.g. adult mental health, GPs, police, adult safeguarding) and non-statutory bodies (e.g. rape crisis, domestic abuse agencies, faith and race-based support organisations, Revenge Porn Helpline). Expectations of external agencies are clearly defined, as are lines of communication and when they should be involved in online safeguarding incidents, so that governance can be applied in a consistent manner. Consideration should be made to link university leads with the local adult safeguarding board where appropriate.	
e. Regulations for students/ student code of conduct/ acceptable usage policy This defines expectations of student behaviour and is signed by enrolling students. The code of conduct should clearly state the expectations of students online as well as offline, and the consequences of failing to adhere to these standards.	**Level 1 — Basic** There is a basic code of conduct in place to cover expectations of student behaviour online and offline, and the consequences of failing to meet such expectations.	
	Level 2 — Embedded There is a code of conduct in place to cover expectations of student behaviour online and offline, and the consequences of failing to meet such expectations. Policy is detailed in terms of expectations and sanctions. Stakeholders are aware of the code and how it can be applied.	
	Level 3 — Holistic There is a code of conduct is in place to cover expectations of student behaviour online and offline, and the consequences of failing to meet such expectations. Policy is detailed in terms of expectations and sanctions. Stakeholders are aware of the code and how it can be applied. The code is informed by emerging trends and student disciplinary data, and is frequently reviewed and updated. Students are kept informed of these updates.	

1. Policy related features (continued)		Our level
f. Safeguarding policy Online safeguarding should be included either within the university safeguarding policy or as a standalone 'online safeguarding policy'. The safeguarding policy should be the overarching policy relating to core expectations around online safeguarding. The policy should determine university definitions of behaviours, such as online abuse and harassment, image-based abuse, identity fraud and exploitation. It should detail expected standards of conduct across staff and student bodies, alongside sanctions for those who breach these standards.	**Level 1 — Basic** A basic policy is in place to meet the requirements of online safeguarding. It includes definitions of online issues such as harassment, image-based abuse, identity fraud and exploitation. It details how the university will respond to safeguarding concerns.	
	Level 2 — Embedded A detailed policy is in place to meet the requirements of online safeguarding. It includes definitions of online issues such as harassment, image-based abuse, identity fraud and exploitation. It details how the university will respond to safeguarding concerns. Policies that include image-based abuse (a specific form of online abuse that relates to the non-consensual sharing of indecent or sexual images by members of the institution) should clearly consider the levels of intervention and sanction for image-based abuse, thresholds for law enforcement intervention, and student support for victims of this form of harm. The safeguarding policy refers to other policies such as student and staff code of conduct/acceptable use, bullying, dignity at work/study policies and disciplinary procedures. Stakeholders are aware of the policy and how it can be applied.	
	Level 3 — Holistic A detailed policy is in place to meet the requirements of online safeguarding. It includes definitions of online issues such as harassment, image-based abuse, identity fraud and exploitation. It details how the university will respond to safeguarding concerns. Policies that include image-based abuse (a specific form of online abuse that relates to the non-consensual sharing of indecent or sexual images by members of the institution) should clearly consider the levels of intervention and sanction for image-based abuse, thresholds for law enforcement intervention, and student support for victims of this form of harm. The safeguarding policy refers to other policies such as student and staff code of conduct/acceptable use, bullying, dignity at work/study policies and disciplinary procedures. The policy is informed from multi-stakeholder input, including external stakeholders. Stakeholders are aware of the policy and how it can be applied. The policy is regularly reviewed by a multi-stakeholder committee using data collected by the university on safeguarding incidents. Policy relates to other aspects of university practice, such as student well-being, and engages readily with both internal (SU, chaplaincy, counselling) and external stakeholders (GPs, adult mental health services, police).	

1. Policy related features (continued)		Our level
g. Staff code of conduct / acceptable usage Policy The policy defines expectations of staff behaviour and is signed by all employees. The code of conduct should clearly state the expectations of staff online as well as offline, and the consequences of failing to adhere to these professional expectations and standards.	**Level 1 — Basic** There is a basic code of conduct in place to cover expectations of staff behaviour online and offline, and the consequences of failing to meet these expectations.	
	Level 2 — Embedded There is a code of conduct in place to cover expectations of staff behaviour online and offline, and the consequences of failing to meet these expectations. Policy is detailed in terms of expectations and sanctions. Stakeholders are aware of the code and how it can be applied. The code is frequently reviewed and updated.	
	Level 3 — Holistic There is a code of conduct in place to cover expectations of staff behaviour online and offline, and the consequences of failing to meet these expectations. Policy is detailed in terms of expectations and sanctions. The policy is informed from multi-stakeholder input, including external stakeholders. Stakeholders are aware of the code and how it can be applied. The code is informed by emerging trends and disciplinary data, and is frequently reviewed and updated.	

2. Education and training related features **These features relate to the development of staff and students' knowledge of online safeguarding, legislation and rights.**		Our level
a. Curriculum Are issues such as online harassment, image-based abuse, hate crime, consent, identity fraud and exploitation, and the relevant associated legislation, considered for all students at the institution? Where appropriate, are relationships between the expectations of professional bodies relevant to the curriculum? Are online behaviours delivered within the curriculum?	**Level 1 — Basic** Information on online safeguarding is given as an induction activity by course leaders or other internal university staff, and is made available via online platforms and in student information areas (for example notice boards).	
	Level 2 — Embedded Information on online safeguarding is delivered as part of the curriculum for all students. Up to date information is made explicitly available and promoted by course teams. Curriculum includes details of rights and legislation around online abuse, consent matters and issues of bystanderism, where to report, and what to expect in response to incidents.	
	Level 3 — Holistic Information on online safeguarding is delivered as part of the curriculum for all students. Curriculum is informed by emerging research and regularly reviewed. It should also be developed in association with the student body via course representatives and the students' union. Up to date and accessible information is made explicitly available and promoted by the university community. Curriculum includes details of rights and legislation around online abuse, and wider related topics such as data protection and the right to be forgotten. The curriculum should also include where to report and what to expect in response to incidents.	
b. Staff training How and which staff are trained to be aware of online safeguarding issues, and what is the depth of training? What does it cover and how often is it delivered? How does staff training relate to governance structures?	**Level 1 — Basic** Internal staff members deliver online safeguarding as part of new employees' induction. Training informs staff of relevant policies and how to respond to online safeguarding incidents.	
	Level 2 — Embedded Internal staff members deliver online safeguarding as part of new employees' induction. Update training is delivered regularly for staff with safeguarding responsibilities. Training informs staff of relevant policies and how to respond to online safeguarding incidents. All safeguarding-related training (for example Prevent, bystanderism, domestic violence and consent) includes online elements and how these issues can be mitigated. Training highlights how online risks can be recognised and how they can be reported.	
	Level 3 — Holistic Internal staff members deliver online safeguarding as part of new employees' induction. Update training is delivered regularly for staff with safeguarding responsibilities. Resources are made available to all staff so they can update knowledge as part of CPD. Training makes staff aware of relevant policies and how to respond to online safeguarding incidents. All safeguarding-related training (for example, Prevent, bystanderism, domestic violence and consent) includes online elements and how these issues can be mitigated. Training highlights how online risks can be recognised and how they can be reported. Training also includes approaches to rectification of harms, such as use of the Right to be Forgotten. Training links with external stakeholders (for example police, adult social care, public health) and is delivered by them where necessary.	

2. Education and training related features (continued)		Our level
c. Stakeholders (internal) How does the institution link with internal stakeholders (for example students' union, student counselling, student ambassadors, chaplaincy) in dealing with online safeguarding issues?	**Level 1 — Basic** Staff training explains the role of internal stakeholders and signposts support from these groups.	
	Level 2 — Embedded Staff training explains the role of internal stakeholders and signposts support from these groups. Staff are made aware of the services offered by internal stakeholders, and how these can be appropriately applied in the event of an online safeguarding incident. Specific services might align to different statutory responsibilities (for example Prevent) and other safeguarding incidents that may have an online element (for example domestic violence). Staff knows when they should report concerns around online risk and harm, and who to report to.	
	Level 3 — Holistic Staff training explains the role of internal stakeholders and signposts support from these groups. Staff are made aware of the services offered by internal stakeholders, and how these can be appropriately applied in the event of an online safeguarding incident. Specific services might align to different statutory responsibilities (for example Prevent) and other safeguarding incidents that may have an online element (for example domestic violence). Staff knows when they should report concerns around online risk and harm, and who to report to. Staff are aware of the limitations of internal stakeholders and when it is necessary to engage with external bodies in addressing online safeguarding incidents.	
d. Stakeholders (external) In dealing with online safeguarding issues, how does the institution link with external stakeholders (for example police, adult social care, mental health GPs and non-statutory Revenge Porn Helpline, legal services)?	**Level 1 — Basic** Staff training explains the role of external stakeholders and signposts support from these groups.	
	Level 2 — Embedded Staff training explains the role of external stakeholders and signposts support from these groups. Staff are made aware of the services offered by external stakeholders and how these can be appropriately applied in the event of an online safeguarding incident. Specific services might be aligned to different statutory responsibilities (for example Prevent) and other safeguarding incidents that may have an online element (for example domestic violence). Staff knows when they should report concerns around online risk and harm, and who to report to.	
	Level 3 — Holistic Staff training explains the role of external stakeholders and signposts support from these groups. Staff are made aware of the services offered by external stakeholders and how these can be appropriately applied in the event of an online safeguarding incident. Specific services might be aligned to different statutory responsibilities (for example Prevent) and other safeguarding incidents that may have an online element (for example domestic violence). Staff knows when they should report concerns around online risk and harm, and who to report to. Staff have single points of contact with external stakeholders (for example the local adult safeguarding board), and have a track record of working with them to resolve online safeguarding incidents.	

3. Technology related features **The use of technology to tackle online safeguarding issues and concerns. Technology can provide useful tools to proactively manage some aspects of online safeguarding.**		Our level
a. Appropriate filtering/ monitoring The institution's use of tools to monitor internet access across its networks and consider the use of filtering where necessary. Care should be taken to reflect the nature of the users across networks (i.e. generally adult) and the risk of overblocking legal content. However, the systems should be clear in addressing illegal content (for example Internet Watch Foundation's blacklist, Child Abuse Image Content).	**Level 1 — Basic** The institution has filtering and monitoring in place that is appropriate for their student body and user base. Technology exists to block illegal content (e.g. Internet Watch Foundation blacklist) and other 'harmful' content based upon institutional policy. Users are made aware of the monitoring policy and associated sanctions.	
	Level 2 — Embedded The institution has filtering and monitoring in place that is appropriate for their student body and user base. Technology exists to block illegal content (e.g. Internet Watch Foundation blacklist) and other 'harmful' content based upon institutional policy. For example, the protection of access to terrorist material or materials that might lead into terrorism (as defined in the Counter Terrorism and Securities Act 2015). Users are made aware of the monitoring policy and associated sanctions, how and when alerts are raised, and lines of communication in the case of an alert. Users are made aware of clear routes for requesting changes to filtering and monitoring based upon individual needs.	
	Level 3 — Holistic The institution has filtering and monitoring in place that is appropriate for their student body and user base. Technology exists to block illegal content (e.g. Internet Watch Foundation blacklist) and other 'harmful' content based upon institutional policy. For example, the protection of access to terrorist material or materials that might lead into terrorism (as defined in the Counter Terrorism and Securities Act 2015). Differentiated filtering is managed based upon the needs of groups of users, and in some cases may be lifted for all but illegal content (for example for research purposes). Institutional policy is open and transparent and regularly reviewed. Users are made aware of the monitoring policy and associated sanctions, how and when alerts are raised, and lines of communication in the case of an alert. Monitoring is pro-active and responds to breaches of acceptable use, as defined in the institution's policies. Users are made aware of clear routes for requesting changes to filtering and monitoring based upon individual needs.	

3. Technology related features (continued)		Our level
b. Bring Your Own Device How does the infrastructure of the institution manage student and staffs' own devices when added to their networks, ensuring similar levels of monitoring and filtering related to safeguarding? Is technology in place to monitor app-based access, e.g. live streaming?	**Level 1 — Basic** The institution has clear policy defined relating to how individuals use institutional technical resources (for example internet access) via their own personal devices.	
	Level 2 — Embedded The institution has clear policy defined relating to how individuals use institutional technical resources (e.g. internet access) via their own personal devices. The policy defines monitoring and filtering approaches applied to personal devices on institutional networks, and has technology in place to implement this.	
	Level 3 — Holistic The institution has clear policy defined relating to how individuals use institutional technical resources (e.g. internet access) via their own personal devices. The policy defines monitoring and filtering approaches applied to personal devices on institutional networks, and has technology in place to implement this. Filtering and monitoring are cognisant of the requirements of different apps and ensure capacity on the network is not overloaded with excessive demand from personal devices (e.g. live streaming).	
c. Internet of Things (IoT) How the institution manages the broader range of internet-enabled devices that might be used across the university estate and networks, and how to ensure these devices cannot be used for harm. For example, remote access to thermostats, live-streaming drones and tracking devices.	**Level 1 — Basic** The institution has clear policy defined related to how IoT devices (e.g. remote access to thermostats) are managed on university grounds. The policy clearly defines acceptable use around personal devices (e.g. drones, tracking devices) and their use on institutional grounds and across its networks.	
	Level 2 — Embedded The institution has clear policy defined related to how IoT devices (e.g. remote access to thermostats) are managed on university grounds. The policy clearly defines acceptable use around personal devices (e.g. drones, tracking devices) and their use on institutional grounds and across its networks. The policy defines sanctions for the abuses carried out using IoT devices related to safeguarding matters.	
	Level 3 — Holistic The institution has clear policy defined related to how IoT devices (e.g. remote access to thermostats) are managed on university grounds. The policy clearly defines acceptable use around personal devices (e.g. drones, tracking devices) and their use on institutional grounds and across its networks. The policy defines sanctions for the abuses carried out using IoT devices related to safeguarding matters. Staff safeguarding training covers issues related to IoT devices and how they can be used for abuse. Disciplinary processes are cognisant of issues related to abuse using IoT devices and apply sanctions consistently.	

4. Practice related features **These features relate to how the institution engages with online safeguarding on a practical level.**		Our level
a. Student engagement How does the institution make use of the student body in delivering practice related to online safeguarding? Are students represented at all levels of online safeguarding practice?	**Level 1 — Basic** Students are consulted in an ad hoc manner regarding online safeguarding issues and incidents.	
	Level 2 — Embedded Students are included in online safeguarding matters, and their input is sought in the development of policy, curriculum, awareness-raising initiatives and training related to online safeguarding.	
	Level 3 — Holistic Online safeguarding is viewed as a collaborative endeavour between students and the institution. Their views and experiences underpin the development of policy, curriculum, awareness-raising initiatives and training. There is student representation at all levels of practice related to online safeguarding, such as training delivery, dissemination and disciplinary matters.	
b. Online safeguarding committee Does the institution have an online safeguarding committee, or is it part of the general safeguarding committee? What is the membership of the committee?	**Level 1 — Basic** Online issues are occasionally discussed at relevant committees, generally after an incident has occurred and concerns are raised. Students are sometimes represented on these committees.	
	Level 2 — Embedded Online issues and concerns are a standing item on committees; for example, the safeguarding committee, equality and diversity committee, student experience and the SU. Students are consistently represented on these committees.	
	Level 3 — Holistic Online issues and concerns are a standing item on committees, with discussions centred on preventing incidents and monitoring effectiveness of strategies proactively as well as reactively. These committees also have external stakeholder representation in addition to student representation.	

4. Practice related features (continued)		Our level
c. Reporting What provision is there for reporting online safeguarding incidents or concerns across the institution[5]? How are stakeholders made aware of these reporting routes?	**Level 1 — Basic** There is some basic information available on how to report online issues.	
	Level 2 — Embedded There is detailed information about how to report online issues which outlines who reports should be made to and what happens after a report is made. Information is also available in a variety of formats. Reports may be anonymised and reported to committees as part of the monitoring progress.	
	Level 3 — Holistic Students and staff know how and where to appropriately report concerns. The information is regularly updated and mechanisms are in place to ensure that information is up to date. Reports are monitored on an ongoing basis. Used anonymously to inform both new interventions for safeguarding and to increase effectiveness of awareness-raising and staff training on an ongoing basis.	

5 According to UUK (2018:3) 'Importantly, when dealing with allegations that have been made about the conduct of one of its students, universities must have regard to the various duties and obligations that they owe to all of their students including performing contractual obligations, exercising a duty of care, applying the principles of natural justice (i.e. the right to a fair hearing before an impartial decision-maker), complying with equality law duties and upholding human rights'.

See *Guidance For Higher Education Institutions How To Handle Alleged Student Misconduct Which May Also Constitute A Criminal Offence* available from

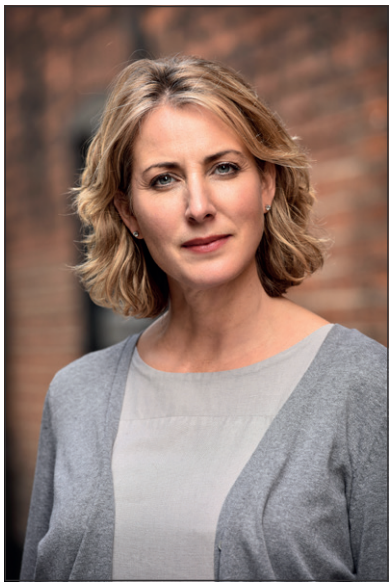
https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2016/guidance-for-higher-education-institutions.pdf

4. Practice related features (continued)		Our level
d. Disciplinary routes How are disciplinary routes applied to online safeguarding incidents? Is the institution clear and transparent with the application of disciplinary policy with regard to online safeguarding?	**Level 1 — Basic** Some information about conduct and acceptable standards of behaviour is available, including potential consequences of failure to meet these obligations. Investigations into allegations of online misconduct are undertaken with due regard to confidentiality. Disciplinary routes for students and staff are in place. They respond to allegations of online misconduct or unacceptable behaviour online.	
	Level 2 — Embedded Detailed information about conduct, acceptable standards of behaviour, and of the likely consequences of failure to meet these obligations is available to staff and students. Timely, objective and thorough investigations into allegations of online misconduct will be conducted with due regard to confidentiality. Disciplinary routes that aim to be fair and consistent in their treatment of students and staff are in place. They aim to be clear and impartial when dealing with allegations of online misconduct or unacceptable behaviour online.	
	Level 3 — Holistic All students and staff are aware of their obligations with regard to conduct, acceptable standards of behaviour, and of the likely consequences of failure to meet these obligations. Timely, objective and thorough investigations into allegations of online misconduct will be conducted with due regard to confidentiality. Disciplinary routes are regularly evaluated to ensure fair and consistent treatment of students and staff. A clear and impartial process is in place for dealing with allegations of online misconduct or unacceptable behaviour online within a reasonable timeframe.	
e. Incident response Does the institution have a clearly defined workflow to address serious incidents related to online safeguarding? Who is made aware of these incident response mechanisms and how are they communicated?	**Level 1 — Basic** The institution responds to serious incidents related to online safeguarding in an ad hoc manner with no clearly defined workflow or replicable process.	
	Level 2 — Embedded The institution has a clearly defined workflow detailing how serious incidents related to online safeguarding should be responded to. A workflow model defines basic processes depending on the nature of the incident and the relationships between offender and victim. It also defines intervention points for referral internally (for example should it be passed to a disciplinary route) and to external agencies (e.g. when to engage with law enforcement).	
	Level 3 — Holistic The institution has a clearly defined workflow detailing how serious incidents related to online safeguarding should be responded to. A workflow model defines clear and well-communicated processes depending on the nature of the incident and the relationships between offender and victim. It also defines intervention points for referral internally (for example should it be passed to a disciplinary route) and to external agencies (e.g. when to engage with law enforcement). All staff and student bodies are familiar with the incident response mechanisms, how they are applied, and where to get help if support is needed.	

4. Practice related features (continued)		Our level
f. Institutional culture Does the institutional culture embrace online safeguarding and reflect student views and experiences? How is this culture represented and promoted across the institution?	**Level 1 — Basic** The institution is considering digital well-being and its responses to online abuse. Some governance is in place and online safeguarding matters discussed at some committees and inductions.	
	Level 2 — Embedded The institution is promoting digital well-being and zero-tolerance of online abuse. This is clearly articulated to students and to staff. There is a governance structure and online safeguarding matters are discussed both formally (for example on committees, inductions and re-inductions, in curricula) and informally (e.g. through clubs, societies, social events).	
	Level 3 — Holistic The institution has a well-established culture of actively promoting digital well-being and zero-tolerance of online abuse. This is clearly and consistently articulated to students and to staff. There is a clear governance structure and online safeguarding matters are reactively and proactively discussed both formally (for example on committees, inductions and re-inductions, in curricula) and informally (e.g. through clubs, societies, social events).	
g. Awareness raising How does the institution raise awareness of online safeguarding and how to recognise concerns? How does it deal with incidents? Does the institution make use of online and offline channels of communication to raise awareness?	**Level 1 — Basic** There are some ad hoc awareness-raising activities taking place, for example, #metoo and hate crime initiatives.	
	Level 2 — Embedded There is a clear and consistent programme of awareness-raising initiatives in place across the university community. The programme covers a range of issues such as revenge porn, indecent images, and coercive control through social media using a variety of traditional and virtual resources (e.g. posters, leaflets, videos and links). This appears in some course curricula.	
	Level 3 — Holistic There is a clear and consistent programme of awareness-raising initiatives in place across the university community that is regularly updated and evaluated. The programme, additionally informed by monitoring reporting and wider concerns, covers a range of issues such as revenge porn, indecent images, and coercive control through social media using a variety of traditional and virtual resources (e.g. posters, leaflets, videos and links). Online safeguarding is including in all course curricula at every level.	

4. Practice related features (continued)		Our level
h. Counselling and student support services Are these services well-briefed on online safeguarding concerns and incidents? Are online safeguarding concerns part of an initial assessment when students engage with these services?	**Level 1 — Basic** Counsellors have some understanding of online safeguarding strategies and recognising online abuse, and it is considered in an assessment.	
	Level 2 — Embedded Counsellors have been trained in assessing digital well-being and in handling disclosures of online abuse. They can advise on online safeguarding strategies and recognising online abuse. Assessment includes consideration of online elements, digital well-being, relationships, screen time, use of technology and a critical consideration of apps and platforms regularly used.	
	Level 3 — Holistic Counsellors have regular training in assessing digital well-being and in handling disclosures of online abuse. They can advise on online safeguarding strategies and recognising online abuse. Sessions actively monitor online issues for progress/deterioration. Assessment includes a detailed consideration of online elements, digital well-being, relationships, screen time, use of technology and a critical consideration of apps and platforms regularly used. Sessions may also include consideration of positive uses of technology to manage risk.	
i. Monitoring and evaluation of policy and practice How does the institution know that its approach to online safeguarding is effective? Does the institution collect any data on their online safeguarding policy and practice? Do they have formal feedback/review/improve mechanisms related to online safeguarding?	**Level 1 — Basic** There is some basic monitoring and evaluation of policy and practice in place.	
	Level 2 — Embedded There is regular monitoring and evaluation of policy and practice in place. Responsibility for reporting these evaluations to committees has been designated.	
	Level 3 — Holistic There is clear oversight, and those responsible for monitoring and evaluating are sure of their roles and responsibilities. There is a clearly communicated, transparent mechanism which includes monitoring of equality and diversity in online safeguarding, and in the application of relevant policies and practices. These processes directly inform continuous improvement for online safeguarding across the institution.	

Biographical details



Professor Emma Bond is Director of Research, Head of the Graduate School and Professor of Socio-Technical Research at the University of Suffolk. She has extensive research experience focusing on online risk and vulnerable groups, especially in relation to domestic abuse, revenge pornography, sexual abuse and image based abuse. Emma has 17 years teaching experience on social science undergraduate and post-graduate courses and is a Senior Fellow of the Higher Education Academy. Her research on virtual environments, mobile technologies and risk has attracted much national and international acclaim and she has been interviewed for BBC Breakfast, ITV, The Today Programme on Radio 4, Woman's Hour on Radio 4, Channel 4's Sex Education Show and for various national media channels in the UK, America and Canada.

Contact: e.bond@uos.ac.uk

Professor Andy Phippen is a Professor of social responsibility in Information Technology at the University of Plymouth and is a Visiting Professor at the University of Suffolk. He has specialised in the use of ICTs in social contexts for over 15 years, carrying out a large amount of grass roots research on issues such as attitudes toward privacy and data protection, internet safety and contemporary issues such as sexting, peer abuse and the impact of digital technology on wellbeing. He has presented written and oral evidence to parliamentary inquiries related to the use of ICTs in society, is widely published in the area and is a frequent media commentator on these issues.

Contact: andy.phippen@plymouth.ac.uk

Useful links

- You can report **online abuse or illegal activity at** https://support.google.com/sites/answer/116262?hl=en
- **Content linked to terrorism can be reported to** https://www.gov.uk/report-terrorism
- You can anonymously and confidentially report **child sexual abuse content, criminally obscene adult content and non-photographic child sexual abuse images** via https://www.iwf.org.uk/
- If someone has been a **victim of revenge pornography, this helpline can provide advice and get images removed** https://revengepornhelpline.org.uk/
- Reporting **indecent or offensive content on Twitter** https://support.twitter.com/articles/15789
- Reporting **indecent or offensive content on YouTube** https://www.youtube.com/intl/en-GB/yt/about/policies/#reporting-and-enforcement
- Reporting **indecent or offensive content on Facebook** https://www.facebook.com/help/contact/274459462613911
- Reporting **indecent or offensive content on Instagram** https://help.instagram.com/519598734752872
- **Hate crime including online content** can be reported via www.report-it.org.uk
- **Harmful or upsetting content can be reported to** https://reportharmfulcontent.com
- If you have been the **victim of fraud contact** https://www.cifas.org.uk **or if you wish to report any form of cybercrime contact** www.actionfraud.police.uk/
- GDPR and Safeguarding https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

University of Suffolk

Published by University of Suffolk

978-1-913160-00-5 Paperback