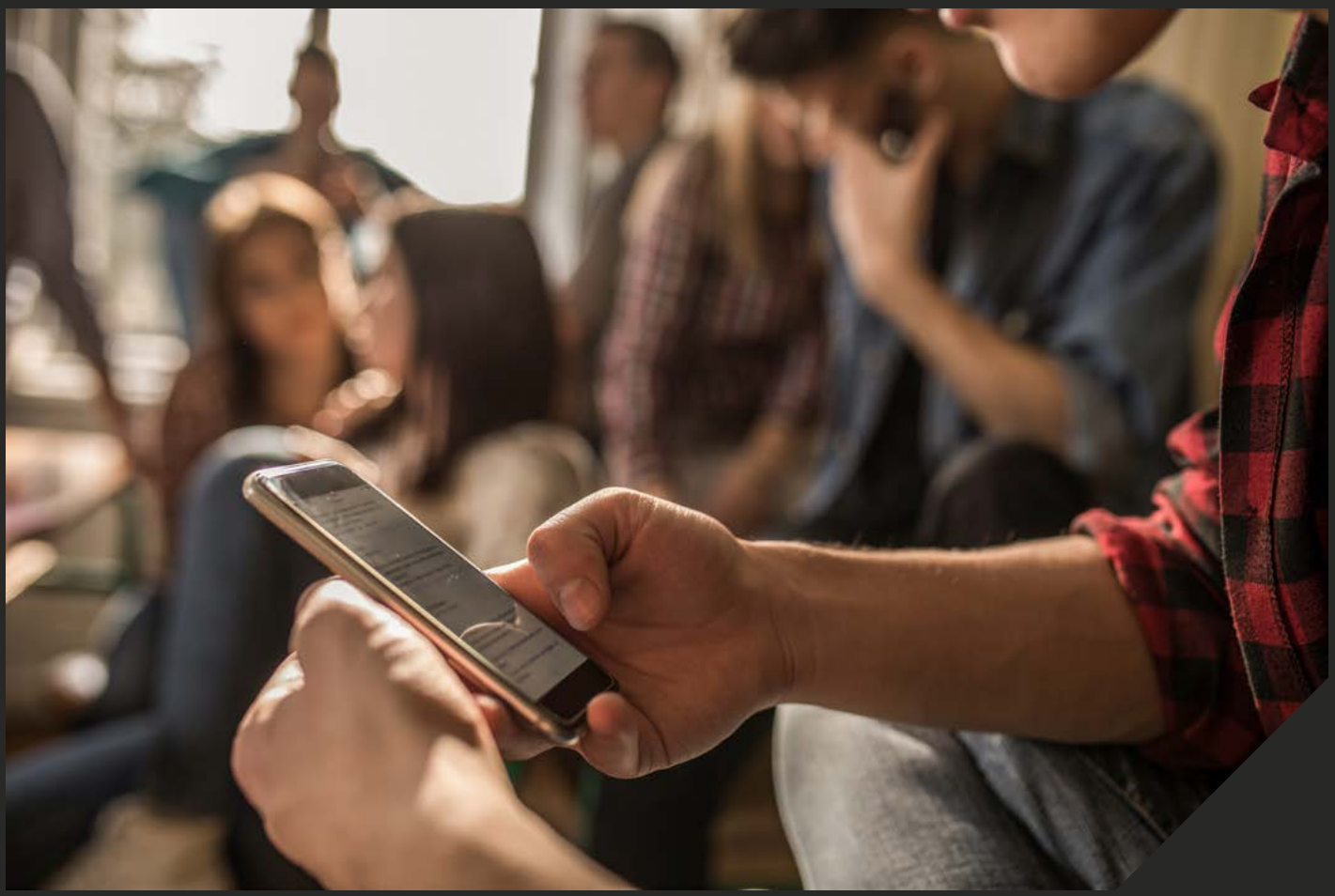
University of Suffolk

HIGHER EDUCATION ONLINE SAFEGUARDING SELF-REVIEW TOOL

2019

By Professor Emma Bond and Professor Andy Phippen



Introduction

Whilst student safeguarding is a well-established responsibility for Higher Education Institutions (HEIs) in the UK, good practice in online safeguarding is only recently becoming recognised across the sector. The launch of the Universities UK (UUK) '*Changing the Culture*' report (UUK, 2016)[1] , which examined the experiences of violence against women, hate crime and harassment affecting university students, called for further action to tackle specifically online harassment and hate crime. Online harms, 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*', do not necessarily cease when young people enter into late adolescence and early adulthood. However, in spite of a duty of care accorded to universities in the UK to act reasonably in students' best interests, to protect their wellbeing and provide support whilst they remain in the education system (UUK, 2017)[4], there remains a dearth of guidance in relation to current practice and regulation around online safety within the higher education sector.

The tool, developed by the University of Suffolk, as part of the Office for Students Catalyst funded programme to support good practice to safeguard students focuses on tackling sexual violence, hate crime and online harassment and is designed for HEIs 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 (HEIs). Each feature can be self-assessed at 4 levels, graded from 0 to 3.

The levels are defined as:

Level	Definition
Level 0 – Reactive	There is no policy/practice in place, and issues are dealt with only in a reactive manner
Level 1 – Basic	There is a basic or minimal definition of policy or fundamental aspects of practice, but they are not detailed in scope or scale or embedded in routine practice.
Level 2 – Embedded	Policy and practice are embedded and students 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 sharing across the HEI 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 policy and practice in place to respond to incidents as they occur, which strive to be effective in response, in a timely and appropriate manner.
Level 2 – Embedded	The institution has policy and established practice in place that in embedded across the organisation such that is can be pro-active and pre-emptive to online safeguarding incidents as well as responding in an appropriate and effective manner.
Level 3 - Holistic	The institution has a well-established and clearly communicated culture across the organisation. Policy and practice is progressive and pro-active, and deals with online safeguarding incidents in a pre-emptive manner. The policy and practice of the incident response and considers broad aspects to prevention such as wellbeing and resilience.

1. Policy related features **The list below is not prescriptive – some institutions will have policies named differently that address the features below. The example terminology is advisory only, and there are many other policies into which these features fit or can be combined (for example, anti-bulling 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 bulling 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. If should also specify how the university will respond to bullying and harassment concerns.	
	Level 2 — Embedded A detailed policy is in place and easily accessible online to meet the requirements of bullying and harassment. 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 and easily accessible online 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. 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. Stakeholders are aware of the policy and how it can be applied. The policy is regularly reviewed by a multi-stakeholder committee based upon data collected by the university on bullying and harassment incidents. Policy relates to other aspects of university practice such as student wellbeing and engages readily with internal (SU, chaplaincy, counselling) and external (GPs, adult mental health services, police) stakeholders.	

1. Policy related features (continued)		Our level
b. Data Protection How does the institution manage data related to student and staff-related safeguarding issues, and 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 are easily accessible online and 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 are easily accessible online and 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 is updated as a result.	
c. Equality and Diversity Policy There may be elements within the Equality and Diversity Policy that relate to hate crime, which may have online elements which need to be considered. Specifically, consideration needs to be made around students with "protected characteristics" which include age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race and ethnicity, religion or belief, sexual orientation. Acknowledgement should be made in the policy to how protected characteristics may place them 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 is easily accessible online and considers online elements to hate crime in detail and how the institution responds to them. 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 and why they should be tackled in order to incorporate equality and diversity and hate crime legislation. Consideration is given in policy to escalating online hate incidents to other agencies (e.g. police).	
	Level 3 — Holistic The Equality and Diversity Policy is easily accessible online and considers online elements to hate crime in detail and how the institution responds to them and has prevention strategies in place through awareness raising 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 and why they should be tackled in order to incorporate equality and diversity and hate crime legislation. Consideration is given in policy to escalating online hate incidents to other agencies (e.g. police). Policy relates to other aspects of university practice such as student wellbeing and engages readily with internal (SU, chaplaincy, counselling) and external (GPs, adult mental health services, police) stakeholders.	

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, student union, external statutory partners (e.g. adult mental health, GPs, Police, adult safeguarding), non-statutory bodes (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, staff members in those roles, and the expectations of those roles. Clear lines of communication are defined so those in the roles know to whom they report on online safeguarding matters.	
	Level 2 — Embedded There is a structure in place that identifies key roles in online safeguarding across the University, staff members in those roles, and the expectations of those roles. Clear lines of communication are defined so those in the roles know to whom they report on online safeguarding matters. The structure should also include external stakeholders from both statutory (e.g. adult mental health, GPs, Police, adult safeguarding) and non-statutory bodes (e.g. rape crisis, domestic abuse agencies, faith and race based support organisations, revenge porn helpline) services.	
	Level 3 — Holistic There is a structure in place that identifies key roles in online safeguarding across the University, staff members in those roles, and the expectations of those roles. Clear lines of communication are defined so those in the roles know to whom they report on online safeguarding matters. The structure should also include external stakeholders from both statutory (e.g. adult mental health, GPs, Police, adult safeguarding) and non-statutory bodes (e.g. rape crisis, domestic abuse agencies, faith and race based support organisations, Revenge Porn Helpline) services. Expectations of external agencies are clearly defined, as are lines of communication and when they should be involved in online safeguarding incidents, such that governance can be applied in a consistent manner. Consideration should be made to link university leads with Local Adult Safeguarding Board where appropriate.	
e. Regulations for Students/ Student code of conduct/ Acceptable Usage Policy Defines expectations of student behaviour that 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 for failing to meet these expectations.	
	Level 2 — Embedded There is a code of conduct in place and easily accessible which covers expectations of student behaviour online and offline and the consequences for 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.	
	Level 3 — Holistic There is a code of conduct in place and easily accessible which covers expectations of student behaviour online and offline and the consequences for 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 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 stand along "Online safeguarding policy". The safeguarding policy should be the overarching policy relating to core expectations around online safeguarding. The policy should define university definitions of behaviours such as online abuse and harassment, image-based abuse, identity, fraud and exploitation and 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 such as harassment, image-based abuse, identity, fraud and exploitation and details how the university will respond to safeguarding concerns.	
	Level 2 — Embedded A detailed policy is in place and easily accessible which meets the requirements of online safeguarding. It includes definitions of online issues such as such as harassment, image-based abuse, identity, fraud and exploitation and details how the university will respond to safeguarding concerns. Policies that include image-based abuse (a specific form of online abuse that related 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 and easily accessible which meets the requirements of online safeguarding. It includes definitions of online issues such as such as harassment, image-based abuse, identity, fraud and exploitation and details how the university will respond to safeguarding concerns. Policies that include image-based abuse (a specific form of online abuse that related to the non-consensual sharing of indecent or sexual images by members of the institution) should clearly consider the levels of intervention and sanction, 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 based upon data collected by the university on safeguarding incidents. Policy relates to other aspects of university practice such as student wellbeing and engages readily with internal (SU, chaplaincy, counselling) and external (GPs, adult mental health services, police) stakeholders.	

1. Policy related features (continued)		Our level
g. Staff code of conduct / Acceptable Usage Policy Defines expectations of staff behaviour that 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 for failing to meet these expectations.	
	Level 2 — Embedded There is a code of conduct in place and easily accessible which covers expectations of staff behaviour online and offline and the consequences for 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 and easily accessible which covers expectations of staff behaviour online and offline and the consequences for 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 knowledge in the staff and student body regarding 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 expectations of professional bodies relevant to curriculum, and online behaviours, delivered within the curriculum?	**Level 1 — Basic** Information on online safeguarding is given as induction activity by course leads or other internal university staff and 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 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 expectations of professional bodies relevant to curriculum, and online behaviours, delivered within the curriculum?	**Level 1 — Basic** Online safeguarding is delivered as part of induction for new employees by internal staff members. Training makes staff aware of relevant policies and incident response to online safeguarding incidents.	
	Level 2 — Embedded Online safeguarding is delivered as part of induction for new employees by internal staff members. Update training is delivered regularly for staff with safeguarding responsibilities. Training makes staff aware of relevant policies and incident response to online safeguarding incidents. All safeguarding related training (for example, Prevent, bystanderism, domestic violence and consent) include 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 Online safeguarding is delivered as part of induction for new employees by internal staff members. 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 incident response to online safeguarding incidents. All safeguarding related training (for example, Prevent, bystanderism, domestic violence and consent) include 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), where necessary, is delivered by external stakeholders.	

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** Training for staff makes them aware of the role of internal stakeholders and signposts support from these groups.	
	Level 2 — Embedded Training for staff makes them aware of 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 be aligned to different statutory responsibilities (for example, Prevent) and other safeguarding incidents that may have an online element (for example, domestic violence). Staff know when and to whom they should report concerns around online risk and harm.	
	Level 3 — Holistic Training for staff makes them aware of 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 be aligned to different statutory responsibilities (for example, Prevent) and other safeguarding incidents that may have an online element (for example, domestic violence). Staff know when and to whom they should report concerns around online risk and harm 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) 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) in dealing with online safeguarding issues?	**Level 1 — Basic** Training for staff makes them aware of the role of external stakeholders and signposts support from these groups.	
	Level 2 — Embedded Training for staff makes them aware of 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 know when and to whom they should report concerns around online risk and harm.	
	Level 3 — Holistic Training for staff makes them aware of 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 know when and to whom they should report concerns around online risk and harm Staff have single points of contact with external stakeholders (for example, 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, IWF watchlist).	**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 (for example, IWF watchlist) made 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 (for example, IWF CAIC list) and other "harmful" content, based upon institutional policy, such as the protection of access to terrorist material or materials that might lead them 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 is the case of an alert. Users are made aware of clear routes for requesting changes to filtering and monitoring based upon individual need.	
	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 (for example, IWF CAIC list) and other "harmful" content, based upon institutional policy, such as the protection of access to terrorist material or materials that might lead them 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 is 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 need.	

3. Technology related features (continued)		Our level
b. BYOD **(Bring your own device)** How does the infrastructure of the institution manage student and staff's 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, for example, live streaming?	**Level 1 — Basic** The institution has clearly defined policy related to how individuals make use of institutional technical resources (for example, internet access) via their own personal devices.	
	Level 2 — Embedded The institution has clearly defined policy related to how individuals make use of institutional technical resources (for example, 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 clearly defined policy related to how individuals make use of institutional technical resources (for example, 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 policy. Filtering and monitoring are conscious of the requirements of different apps and ensure capacity on the network is not overloaded with excessive demand from personal devices (for example, 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, livestreaming drones, tracking devices?	**Level 1 — Basic** The institution has clearly defined policy related to how "Internet of Things" devices (for example, remote access to thermostats) are managed on the university estate. The policy clearly defines acceptable use around personal devices (for example, drones, tracking devices) and their use on institutional estate and across its networks.	
	Level 2 — Embedded The institution has clearly defined policy related to how "Internet of Things" devices (for example, remote access to thermostats) are managed on the university estate. The policy clearly defines acceptable use around personal devices (for example, drones, tracking devices) and their use on institutional estate 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 "Internet of Things" devices (for example, remote access to thermostats) are managed on the university estate. The policy clearly defines acceptable use around personal devices (for example, drones, tracking devices) and their use on institutional estate 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 conscious of issues related abuse using IoT and apply sanctions consistently.	

4. Practice related features **These features relate to how the institution engages with online safeguarding at 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 discussed at relevant committees on an ad hoc basis 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 to whom the reports are made and what happens after a report is made. A variety of reporting mechanisms including face-to-face and online are available. 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. A variety of reporting mechanisms including face-to-face and online are available. Online reporting is open and transparent with clearly defined polices regarding confidentiality of all parties and the lawful processing of information collected in the reporting process. The information is regularly updated and mechanisms are in place to ensure that that information is up-to-date. Reports are monitored on an ongoing basis and used anonymised to inform both new interventions for safeguarding and the 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

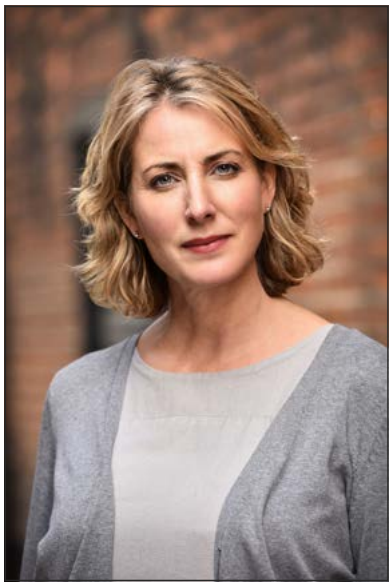
https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2016/guidance-for-higher-education-institutions.pdf

4. Practice related features (continued)		Our level
d. Disciplinary routes 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** Some information about conduct and acceptable standards of behaviour is available which includes potential consequences of failure to meet these obligations. Investigations into allegations of online misconduct are undertaken with due regard to confidentiality. Discipline routes for students and staff are in place. They respond to allegations of online misconduct or unacceptable behaviour online.	
	Level 2 — Embedded Online issues and concerns are a standing item on committees, for example, detailed information about conduct and acceptable standards of behaviour, and the likely consequences of failure to meet these obligations is available to staff and students. Investigations into allegations of online misconduct will be carried out in a timely, objective and thorough manner, with due regard to confidentiality. Discipline routes which 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 and acceptable standards of behaviour, and the likely consequences of failure to meet these obligations. Investigations into allegations of online misconduct will be carried out in a timely, objective and thorough manner, with due regard to confidentiality. Discipline 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 time frame.	
e. Incident Response What provision is there for reporting online safeguarding incidents or concerns across the institution? How are stakeholders made aware of these reporting routes?	**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 and intervention points for referral internally (for example, should it be passed to a disciplinary route) and to external agencies (for example, 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 and intervention points for referral internally (for example, should it be passed to a disciplinary route) and to external agencies (for example, 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 What provision is there for reporting online safeguarding incidents or concerns across the institution? How are stakeholders made aware of these reporting routes?	**Level 1 — Basic** The institution is considering digital wellbeing 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 wellbeing and zero-tolerance of online abuse which is clearly articulated to students and to staff. There is a governance structure and online safeguarding matters discussed both formally on committees, inductions and re-inductions, curricula and informally through clubs, societies, social events.	
	Level 3 — Holistic The institution has a well- established culture of actively promoting digital wellbeing and a zero-tolerance of online abuse which 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 on committees, inductions and reinductions, curricula and informally through clubs, societies, social events.	
g. Awareness raising What provision is there for reporting online safeguarding incidents or concerns across the institution? How are stakeholders made aware of these reporting routes?	**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, for example, revenge porn, indecent images, coercive control through social media using a variety of traditional and virtual resources e.g. posters, leaflets, videos and links to further information and support and through some course curricula.	
	Level 3 — Holistic There is a clear and consistent programme of awareness raising initiatives in place across the university community which is regularly updated and evaluated. The programme, additionally informed by monitoring of reporting and wider concerns, covers a range of issues, for example, revenge porn, indecent images, coercive control through social media using a variety of traditional and virtual resources e.g. posters, leaflets, videos and links to further information and support. Online safeguarding is including in all course curricula at every level.	

4. Practice related features (continued)		Our level
h. Counselling and student support services What provision is there for reporting online safeguarding incidents or concerns across the institution? How are stakeholders made aware of these reporting routes?	**Level 1 — Basic** Counsellors have some understanding of online safeguarding strategies and recognising online abuse. Assessment includes consideration of online abuse.	
	Level 2 — Embedded Counsellors have been trained in assessing digital wellbeing 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 wellbeing, 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 wellbeing and in handling disclosures of online abuse. They can advise on online safeguarding strategies and recognising online abuse and sessions actively monitor online issues for progress/deterioration. Assessment includes a detailed consideration of online elements, digital wellbeing, 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 What provision is there for reporting online safeguarding incidents or concerns across the institution? How are stakeholders made aware of these reporting routes?	**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 with designated responsibility for reporting of such to committees.	
	Level 3 — Holistic There is clear oversight and the duty to monitor and evaluate clearly outlines with roles and responsibilities. There is a clearly communicated, transparent mechanism with included 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, 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** https://support.google.com/sites/answer/116262?hl=en
- Reporting **content linked to terrorism** 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** https://www.iwf.org.uk/
- If someone has been a **victim of revenge pornography, the 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 wish to report any form of cyber crime contact** www.actionfraud.police.uk/
- GDPR and Safeguarding https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf