Internet & E-Mail Abuse
Mapping The Legal Minefield For Academies

In this White Paper, noted Legal Expert Dr. Brian Bandey discusses the overall Threat Landscape that e-Safety Law produces for the Academy with respect to both of its roles – firstly as a corporate employer; and secondly as an educational institution. He identifies in general terms the different doctrines of Law that apply when the Academy provides both Employees and Pupils with access to ICT and they misuse it.

Dr. Bandey pinpoints the manner in which Legal Obligations and Law-Based Liability (from both Employee and Pupil) attach to the Academy in a more comprehensive, direct and penetrative fashion – compared to the Local Authority controlled School who is often neither the Employer nor the owner of School Premises. In doing so, Dr. Bandey makes reference to more detailed Smoothwall White Papers available at: http://www.smoothwall.net/resources/white-papers.

EXECUTIVE SUMMARY

Internet & E-Mail Abuse - Mapping The Legal Minefield For Academies

Additional Areas of e-Safety Law are Applicable to the Academy.

Unlike a Local authority controlled School – the Academy is an Employer and a Land-Owner. As such additional areas of Law which attach to e-Safety and e-Safeguarding (both of Staff and Pupils) arise. Most education management teams are usually not well-accustomed to measuring, accommodating and taking decisions on forms of Exposure that are exclusively Law-Based are usually arise exclusively in the Corporate Sector.

e-Safety Obligations are Not Delegable.

The e-Safety Law Obligations, Duties and Responsibilities that fall on the Academy and its Officers and Managers are Non-Delegable.

The Absence of the Local Authority.

Certain Obligations and Duties – especially those arising under the Occupier Liability Acts and the Health & Safety Acts (as either Employer or Premises Owner) previously fell to the Officers and Managers of the Local Authority. These now fall and focus upon the Officers and the Managers of The Academy Trust. Those Officers and Managers may find themselves personally legally exposed for breaches of such duties.

The Inefficacy of Insurance.

Great emphasis has been placed elsewhere on the need of the Academy Trust to put in place professional indemnity and other insurances to protect its Members, Officers and Managers. That is not all the story. Health & Safety Law and Child Protection Law still has the power to make Officers Personally Liable and to Prosecute them. Exposure to Legal Proceedings often means the Destruction of Careers.

Offensive and Obscene SPAM.

Employers are liable to their Employees if they do not take reasonable and practical steps to protect them from receiving Indecent, Offensive or Obscene SPAM.

Sexual Harassment.

Employers are being sued by Employees who have been sexually harassed or bullied both through seeing inappropriate images and through co-workers misusing their Employer's E-Mail and Internet Access facilities.

Statutory Defences.

Employers can use legal statutory defences when sued by an Employee who have been sexually or racially harassed through the misuse of E-Mails and Internet Access by taking all reasonably practical measures to avoid the act complained of. Active Supervision Technologies are a reasonably practical measure.

Harassment in General.

Employers are Legally Liable to an Employee who has been Harassed by another Employee.

Vicarious Liability.

An Employer's only defence where is it Vicariously Liable for an Employee's misdeeds is Interception (preventing the harassment via the e-mailing in the first place).

Pornography in the Workplace.

Employers are being sued by Employees who have been exposed to Pornographic Internet Content being accessed by their co-workers.

Corporate Defamation.

Employers have found themselves liable for hundreds of thousands of pounds worth of damages when their Employees libel a competitor via E-Mail.

Reputational Loss.

Credibility in the market-place is being seriously lost when it becomes public that Employees engage in Inappropriate Internet Use which involve Explicit Images.

Criminal Prosecution.

Employers may suffer Criminal Prosecution when employees disseminate Pornography using the employer IT infrastructure.

Child Pornography.

Employers may suffer Criminal Prosecution if they neglect to prevent Employees from downloading Child Pornography into the workplace from the Internet using the employer IT infrastructure.

Technology Changes Legal Thresholds.

It should be understood that the advent of accessible, affordable and reasonably reliable Active Supervision Technologies lowers the Threshold of Legal Liability in the context of e-Safety for the Academy.

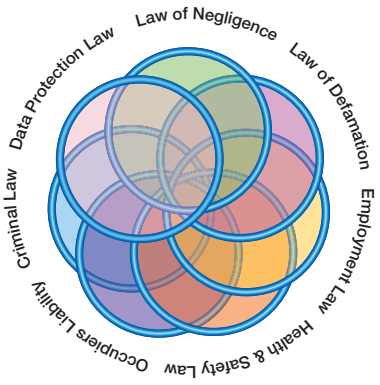
1. Introduction

In this Briefing Paper I will be seeking to both highlight and give a high-level overview of the "dualism" that exists for the Academy with respect to its e-Safety Law obligations. The Academy is now the employer of teaching, administrative and support staff and is also the owner of Academy property (both real and personal). The Academy is, in Law, a form of Corporation and exists as a Legal Person as such.

Only a Legal Person can sue and be sued.

The Academy HazardSphere™ as Employer and School

The Law produces a number of overlapping Doctrines of Law which intersect over the activities concerned with the e-Safety of Employees and Pupils as they use the Academy's ICT and, indeed, misuse it. Misuse it to access and download pornography – misuse it to bully, harass and threaten each other – misuse it to access sites inappropriate for their age (with all of the emotional, developmental and behavioural problems that can flow). Below is a sketch diagram to illustrate such an 'intersection' the centre of which is a hazardous and turbulent area.



The title to this Briefing Paper includes: "Mapping the Legal Minefield for Academies" and it is only going to be a 'Sketch Map'. Not all areas will be addressed and those that are addressed will only be done so superficially. Having said that, I am trying to achieve here a new entrée for Academy Management into the duality of their e-Safety Legal Obligations. One area facing towards their Employees – one area facing towards Pupils; but these two areas overlapping in an asymmetric fashion.

So in order to sketch the map I have crudely divided the matter into two areas. The first (Section 2.) addresses the Legal Exposure caused to the Academy when its Employees misuse the e-mail and Internet access systems it provides for them. It also parses some of the positive obligations flowing from Academy to Employee – with respect to e-Safety Law.

The second (section 3.) is directed more to the e-Safeguarding obligations of the Academy towards its Students (who, in most cases, will be minors). In very much the same way as an Employer, the Academy as School requires Pupils to use its ICT. But children are not the same as adults – and the Law recognises this full well.

The Law recognises that minors are not only inherent risk-takers; but developmentally unable to anticipate accurately the consequences of the risks they take.

The Law similarly recognises that a "KEEP OUT" sign is as much an attraction to one child as it would be a deterrent to another.

Thus the Thresholds of Legal Liability are significantly lowered as between Academy " Pupil; compared to Academy " Employee.

Finally, the reader ought to be aware that I have elected not to parse some areas of e-Safety Law at all.

2. The Academy as Corporate Employer – Employee Misuse of Academy ICT ~ Internet & E-Mail

Explicit Images and E-Mail Text causing Harassment

What Amounts to Harassment?

Any form of sexual harassment is capable of amounting to unlawful discrimination for which the employer will be liable. E-Mails containing Explicit Images or the showing of Explicit Images, for example sexual images sent in an E-Mail, fall squarely into this arena. The key element that dictates whether or not conduct amounts to harassment is whether the victim finds the conduct in question unwelcome. Thus it is irrelevant if another employee considers the same E-Mail content or image to be amusing or otherwise inoffensive; the point is that if an employee finds the content or image offensive, and if the material in it is sexual, then it becomes unlawful harassment.

Where harassment is sexual in nature, the victim would be able to take a claim of unlawful discrimination to an employment tribunal and these Courts have taken the view consistently over a period of many years that sexual harassment is capable of causing a injury to the employee and is thus a form of unlawful discrimination. The same principles apply to racial and disability harassment.

A little known legal truth is that the ***Prevention*** of an event which would otherwise give rise to a legal right to sue is far, far better than defending the action later.

The new generation of Active Supervision Technologies permit, for the first time, the prevention of sexual harassment through digital means.

What is the definition of Sexual Harassment?

The legislation expressly states that sexual harassment is unlawful and provides that a person subjects another to harassment if:

(i) on the ground of sex, a person engages in unwanted conduct that has the purpose or effect of violating the other person's dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment.

For example – an employee regularly downloading pornographic pictures of women onto his computer could have the effect of creating a degrading environment for a woman to work in.

(ii) a person engages in any form of unwanted verbal, non-verbal or physical conduct of a sexual nature that has the purpose or effect of violating the other person's dignity or of creating an intimidating, hostile, degrading, humiliating or offensive environment.

For example – an employee sending pornographic images to another by e-mail would fall within this definition.

(iii) on the ground of the other person's rejection of or submission to unwanted conduct of the kind set out in (i) or (ii) above, a person treats another less favourably than they would have treated him/her had s/he not rejected, or submitted to, the conduct.

For example – a manager failing to give an employee an opportunity for promotion because they complained of his lewd e-mail which contained Explicit Images.

A little known legal truth is that the ***Prevention*** of an event which would otherwise give rise to a legal right to sue is far, far better than defending the action later.

The new generation of Active Supervision Technologies1 permit, for the first time, the prevention of sexual harassment through digital means.

1 In this Briefing Paper, the term "Active Supervision Technologies" means Computer software technology which: (i) reads or views Internet based traffic; or (ii) reads or views the content of computer display peripherals (whether the computer is offline or online); and, if such traffic or content meets certain criteria: (a) prevents the intended recipient's access to it; or (b) prevents the display of the content; or (c) automatically generates alerts or reports in respect of such traffic or content.

What if Sexual Harassment wasn't intended?

It is important to note, in the context of discussing the misuse of e-mail and Internet access technology in the workplace, that conduct can have the 'effect' of creating an intimidating, hostile, degrading, humiliating or offensive environment even if creating such an environment was not the intention of the person carrying out the conduct. When assessing whether the conduct has this effect, a tribunal will consider all the circumstances, including the complainant's perception of the alleged harassment and whether it is reasonable to consider the conduct as being a form of harassment.

It can be seen from this that the question of whether or not particular behaviour when using ICT constitutes sexual harassment is a subjective one. This means if a particular employee finds a colleague's conduct offensive, and if the conduct is sexual in nature, then it is by definition unlawful sex discrimination. It is irrelevant whether anyone else thinks that the conduct is not offensive or unreasonable.

Sexual Harassment by Third Parties

An Academy will be potentially liable for sexual or sex-related harassment of its employees by contractors, clients and other third parties, where such harassment takes place in the course of the employee's employment. The Academy will have a defence to such claims provided that it has taken such steps as would have been reasonably practicable to prevent the third party from harassing the employee. The Academy must also know that the complainant has been subject to harassment in the course of his/her employment on at least two other occasions by a third party (whether or not that third party is the same or a different person on each occasion).

In many office environments, employees are actively encouraged to produce good relations with the employees of clients, customers and suppliers. Since much of this interaction now takes place through e-mail; the risk that the Third-Party Employed would misuse the 'relationship' and their employer's e-mail system to 'sexualise' the relationship is now considerably higher. It is suggested that, in order to access the Statutory Defence, one of the key indicators for the harassed's Employer would be the monitoring and interdiction of inbound e-mails so as to control and prevent the entry into the workplace of profane or sexualised e-mails.

The Truth of Employee Behaviour

From recent case law and studying the misuse of ICT at work, it seems that the truth of the matter is this. No matter what "Acceptable Use Policies" are put into place; human behaviour in the modern workplace means that these incidents will invariably occur, costing employers tens of thousands of pounds in legal costs and human resource time. How much better it would be to intercept this behaviour – especially as it often leads to other employees being distressed and being able to sue their employers?

Internet Access and Indirect Harassment

How can Internet Access Amount to Harassment?

Uncontrolled Internet access routinely leads employees into misbehaviour which is, in legal terms, ***sexual harassment***. For example, in one case that went to Court a female employee, who worked in an open-plan office, saw sexually explicit material which her male colleagues regularly downloaded from the Internet and displayed on their workstation monitors. This downloading was not part of their employment but was conducted for their personal 'enjoyment'. She resigned and sued her employer for sex discrimination and sexual harassment.

Even though the activities she complained of were not directed at her personally, and despite the fact she had not previously raised any complaint with management, she won her case. The Court said that the working environment was hostile to her as a woman due to the sexually explicit material being circulated. In this real-life situation, if the employer had implemented a modern Content Security System the pornography may have been blocked – a valuable employee kept who was never exposed to the pornography, and training initiated for those trying to download. Even if the porn filter had let the images through – the employer may very well have had a ***total legal defence***. That is that they had taken all reasonable and practical measures to prevent the harassment.

In this case – the Employer could not have been successfully sued if they had implemented a modern Active Supervision Technology Solution.

Either the downloading of porn would have been prevented, or the Employer would have the defence of taking ***all reasonable practical steps*** to prevent the harassment.

How is the Employer to Blame for this type of Employee Behaviour?

All of the UK Law dealing with discrimination contain makes employers legally liable for their workers' actions in the course of their employment, whether or not the actions in question were done with the employer's knowledge or approval. This means that the employer cannot escape liability by:

- pleading ignorance of the fact that harassment was being suffered by an employee;
- arguing that there was no intent to cause offence to the person affected;
- blaming the employee for failing to complain formally to management about the alleged harassment.

Often the employees who is suffering the harassment may not come forward to a member of management to complain. Where unacceptable e-mail content or images are concerned they often feel particularly embarrassed about what is happening to them, fear that they will not be believed or taken seriously, or worry that a complaint will just cause problems for themselves.

To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the Employer must show they have taken ***all reasonably practical measures*** to prevent it.

Active Supervision Technologies are the newest reasonably practical measures which MUST be taken. Without them – use of the Statutory Defence is more likely to fail completely.

How does the Employer defend itself?

The Law says that the responsibility lies squarely with employers to take all reasonable steps to prevent discrimination (including harassment) from occurring.

To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the Employer must show they have taken all ***reasonably practical measures*** to prevent it.

Active Supervision Technologies are the newest reasonably practical measures which MUST be taken. Without them – use of the Statutory Defence is more likely to fail completely.

So legally, if an employer takes all ***reasonably practical measures*** to prevent discrimination (including harassment) from occurring in the workplace, this will provide what is called a ***Statutory Defence*** in the event that they are sued following an allegation of harassment.

Employers escaping legal liability can be seen to work completely in real life.

In one piece of litigation, the Court decided a case where one of the employees had made racially discriminatory remarks in the presence of another employee who was of Iraqi-Arabic ethnic origin. However, the employer involved had devised and implemented a policy on racial awareness, had made every employee fully aware of the need to abide by the policy, and had carried out training on racial and sexual awareness.

Because of this action, the Court decided that the employer had taken such steps as were reasonably practicable to prevent discrimination from occurring. The Court concluded that the provisions the employer had put in place to ensure racial equality fulfilled the statutory defence and they were therefore not liable at all.

How can Technology Help Provide a Legal Defence?

To use the Statutory Defence against a case where the Employer is being sued for harassment and discrimination, the reasonably practical measures taken ***do not have to be perfect or infallible***.

No technology is 100% accurate or available 24–7. The Law understand this – merely requires its implementation as a reasonably practical measure and that the implementation is not merely for show.

We have seen the that Statutory Defence is only available to the Employer if they can show that they have taken all reasonably practical steps to avoid the harassment. One modern and now common-place step to be taken is the implementation of a modern Active Supervision Technology whereby the software checks e-mails for profanity and indecent or obscene pictures. The Employer must be able to show that if an implementation of this type of technology is reasonably practical in order to protect employees, than they have done so. Thus an implementation of this technology (which is not just for show) will substantially improve an Employer's ability to access this defence.

To use the Statutory Defence the reasonably practical measures taken ***do not have to be perfect or infallible***.

No technology is 100% accurate or available 24–7. The Law understands this – merely requires its implementation as a reasonably practical measure and that the implementation is not merely for show.

What about SPAM?

A great deal of SPAM is rude, lewd or may contain indecent images. Once again the Employee has a right not to work in a hostile workplace where their health is not negatively affected. SPAM can create a hostile workplace as easily as any form of sexual or racial discrimination.

Understanding the Employer's Liability for the Acts and Omissions of its Employees

What is Vicarious Liability?

In broad legal terms, employers are responsible for what their employees do, and what they fail to do, in the course of their employment. This is known as the Doctrine of Vicarious Liability. It follows that any misdeeds committed by workers in the course of their employment can lead to legal claims being successfully taken against the employer by the injured party.

The legal theory of Vicarious Liability even extends to workplace bullying and Employers are liable for workplace harassment even if they were not in any way negligent. With a new generation of workers entering the workplace – who are used to texting, instant messaging and e-mailing; bullying using these digital means is bound to rise.

Previously employees had to prove that the employer was negligent in not stopping bullying taking place and that it had caused them psychological damage. But the law has changed on this point and it means that companies can be sued even if the company cannot be expected to have known about the bullying and this law is certainly wide enough to include the use of Explicit Images and E-Mailing as vehicles for e-bullying.

Vicarious Liability is the no-fault liability where the ***Blameless Employer*** is ***liable*** in law for the acts of the ***Blameworthy Employee***.

We **know** digital Pornography and E-Mails are instruments used to bully and harass in the workplace.

The Interception of such misuse is the **ONLY** defence available in law.

Are there Defences to Vicarious Liability in this Context?

Vicarious Liability is the no-fault liability where the ***Blameless Employer*** is ***liable*** in law for the acts of the ***Blameworthy Employee***.

We **know** digital Pornography and E-Mails are instruments used to bully and harass in the workplace.

The Interception of such misuse is the **ONLY** defence available in law.

There can be no doubt that this law has serious implications for employers as it gives employees who are bullied or harassed at work an additional way to claim compensation from their employers. Moreover, some of the existing limitations and defences will not be available. For example, an employer has a defence under existing discrimination legislation if it can show that it took all reasonably practicable steps to prevent discriminatory harassment occurring. This would not help an employer facing a claim that it was vicariously liable for an employee's harassment under the Prevention from Harassment Act 1997.

As we know that harassment takes place in the workplace through the use of pornographic images and obscene and bullying e-mails, it seems that the only avenue forward for employers in avoiding the breadth of this area of law is to use every means, including technology, to try to intercept e-harassment and the E-Mails or the Explicit Images used by the workplace bully so as to stop it reaching the intended victim.

Employees, Pornography and Obscene Material in General

What if Employees are Forwarding Pornographic E-Mails and Attachments?

One of the most common and difficult problems an employer may face is the discovery that an employee has been using their computer system to access, view, download or transmit pornographic or sexually explicit material. Although the possession or downloading of adult pornography is not a criminal offence under English Law (unless it is obscene or of a paedophilic nature), the transmission or distribution of such material is illegal.

Thus for example, an employee who transmits a pornographic picture to a co-worker or to someone outside the organisation as an E-Mail attachment is committing a criminal offence.

Undoubtedly, the most important aspect of an employer's duty to its employees which is implied by Law is the duty to take reasonable care to ensure the safety of its employees. There are a number of common law rules which determine the extent of that duty, and in addition there are certain statutory provisions designed to ensure the employee's safety which, if broken or not observed by the employer, may lead to an action for damages by an injured employee based on a breach of statutory duties.

What about Offensive or Obscene e-Mails which aren't Pornographic?

It is illegal to send indecent or grossly offensive material in order to cause the recipient distress or anxiety. It is also a criminal offence send over a public electronic communications network a message that is of a "…grossly offensive or of an indecent, obscene or menacing character". This includes the Internet.

Following the expansion of the Doctrine of Vicarious Liability – the likelihood of an employer being vicariously liable for an employee's breach of either the Communications Act 2003 or the Malicious Communications Act 1988 (which produce the crimes just mentioned) must be very considerably higher.

Is it true that Indecent E-Mails in the Workplace can be a Criminal Offence?

What damage will be done to an Employer when an Employee's Indecent E-Mails causes them to be entered on the Sex Offenders' Register?

What are the ***Vicarious Liability*** Issues here?

Once again – Interception is the **ONLY** realistic answer.

Yes – the sending of e-mails of a sexual nature could earn the sender a place on the Sex Offenders' Register offences which are not primarily sexual in nature to be punishable by a Sexual Offences Prevention Order (often referred to as a "SOPO").

Improper use of a public communications network is forbidden already by the Communications Act 2003. It defines improper use as sending a message that is "grossly offensive or of an indecent, obscene or menacing character". The amendment to the Sexual Offences Act add that offence to the list of others that qualify for a SOPO and covers such activities as nuisance phone calls, obscene messages and harassment emails of a sexual nature.

What damage will be done to an Academy when an Employee's Indecent E-Mails causes them to be entered on the Sex Offenders' Register?

What are the ***Vicarious Liability*** Issues here?

Once again – Interception is the **ONLY** realistic answer.

People issued with a SOPO are added to the Sex Offenders' Register. The Register is designed to monitor and control the behaviour of, and therefore the risk posed by, sex offenders. Therefore an Academy employee who sent e-mails, via the Internet, to others could be put on the public UK Register together with rapists and paedophiles.

Employees and Paedophilic Images

Do Paedophiles Download and Keep these Images at Work?

The existence of child pornography on an organisation's computer system may expose the corporation itself (and possibly senior individuals within it) to criminal prosecution. There is now substantial evidence available which shows that the dysfunctional individuals who engage in the downloading and keeping of child pornography, are likely to do that at work also if given unrestricted access to the Internet at their workplace. The lead case on this issue involved a Lecturer at a University. Prudent employers should do their best to intercept such behaviour at it's source since no amount of work-orientated training can restrain an individual from such a behavioural characteristic.

Can the Employer be Liable?

If management (and therefore the corporate employers) are shown to have been 'neglectful' in allowing child pornography into their IT structure; Criminal Liability attaches not only to the company itself but also to its officers and directors (which will be a matter of record). Additionally it applies to "Managers" and persons purporting to act in such a senior capacity. The question of whether or not a person is a "Manager" is a question of Law.

Why are Academy Officers personally exposed to Criminal Prosecution?

As the purpose of the Law is "… *to fix with criminal liability only those who are in a position of real authority, the decision-makers within the company who have both the power and responsibility to decide corporate policy and strategy. It is to catch those responsible for putting proper procedures in place; it is not meant to strike at underlings*" it is constructed so that it is able not only to catch the Employer itself, but is capable of catching those Corporate Officers and their IT Directors, Security Directors and Senior Managers who decide corporate policy and are responsible for putting the proper procedures that will help prevent child pornography infecting their systems.

Remember – these systems that protect the Employer's systems ***do not have to be 100% effective***. Rather, implementing sensible training and systems goes to show that the Employer has not been 'Neglectful'.

Corporations and their Executives will have to put forward sound reasoning, based on legal rules and legal analysis, as to why no "Neglect" had taken place in circumstances where an employee was making (downloading or copying) indecent photographs of children using the Employer computer system where no Active Supervision Technology was present.

Academy Officers and Managers are required by the Law NOT to be Neglectful with respect to the entry points for Child Pornography making its way into their IT Infrastructure.

We know paedophiles download and keep child pornography in the workplace. The legal cases tell us so.

Consequently, Image Interception Technology must be an essential component in every Corporation's legal protection strategy.

3. The Academy as Educational Institution – Pupil Access to Academy ICT ~ Internet & E-Mail

Surely – a School's Obligations in Law with respect to e-Safety are the same? E-Safety Legal Obligations and Liabilities must be identical between Academy and Local Authority controlled School? Well, in one sense they are – but in another they do not.

The legal obligations that fall on the School to e-safeguard the children in its care and the liabilities that arise through a failure to meet e-Safety obligations are often shared between, for example, the School and the Local Authority.

There is no such 'sharing' in the case of Academies. Rather, the Legal Exposure and the Legal Liability becomes focussed exclusively on the Academy Trust and its Managing Officers. Individuals may occupy more than one post contemporaneously – so the Headteacher may be Headteacher (with its own singular legal obligations as to e-Safety), and also occupy positions as a member of the Academy Trust (which may be a position directly responsible for Statutory Health & Safety Obligations including Pupil e-Safety) and may be a Director with similar responsibilities.

Unlike the Local Authority School, the Academy is a self-sufficient Employer Corporation.

So if an Academy Employee is Negligent with respect to e-Safety Law – there is ONLY the Academy to sue.

Health and Safety Law

One of the most important Legal Duties that is placed on the Academy is with respect to the Health and Safety of Pupils whilst in the care of the School.

The United Kingdom Health and Safety Legislation places Statutory Obligations on "Employers" (a matter expanded upon in the relevant Smoothwall White Paper) which cannot be delegated, nor ignored, nor avoided. The only option for the Employer is to satisfy the requirements of Health and Safety Legislation. For the purposes of that legislation - pupils are protected by the duties imposed because they are affected by an Employer's undertaking or are using Academy premises.

Now it is a known fact that Pupils will bully, threaten and intimidate each other using the Academy's IT infrastructure. It is a known fact that Pupils will threaten each other with violence by passing e-messages in the classroom. Similar attempts at extortion have also been discovered which take place, in the classroom and with the teacher present, through the vector of e-messaging using the School's ICT. The psychological, emotional and developmental damage that can be done to a child in such circumstances is similarly well know.

Responsibility for the health and safety of pupils lies with the Governing Body of the Academy, either as the Employer of Academy staff or because it controls Academy premises (or both).

The Education and Inspections Act 2006 places a corresponding duty on Governing Bodies to promote well-being. "Well-being" is defined in the Children Act 2004 in terms of:

- physical and mental health and emotional well-being;
- protection from harm and neglect;
- education, training and recreation;
- the contribution children make to society;
- social and economic well-being.

and these are the five Every Child Matters outcomes:

- being healthy;
- staying safe;
- enjoying and achieving;
- making a positive contribution;
- achieving economic well-being.

The Health and Safety at Work Act 1974 obliges the Academy to have a health and safety policy with respect to the e-Safety of Pupils and obliges the Academy to make arrangements to implement it.

It is expected that Governing Bodies will keep under review the contribution their Academy is making to each of the five outcomes, and satisfy themselves that this contribution is appropriate to the needs of their pupils.

One can also readily see that e-Safety drives directly to the School's obligations under the Children Act 2004; for a child cannot enjoy (for example) mental health and emotional well-being whilst being cyberbullied through the Academy's ICT. Similarly, a child is not being protected from 'harm and neglect' if the Academy itself has not put into place appropriate technologies to manage the Risk in exposure to Illegal and Inappropriate Material on the Internet.

The Health and Safety at Work etc Act 1974 obliges the Employer to have a health and safety policy and arrangements to implement it.

In practice, Academies may delegate specific health and safety tasks to individuals. ***But the Academy retains the ultimate legal responsibility no matter who carries out the tasks.*** The Academy should therefore maintain an audit track, making clear who is doing what and confirming that these tasks are being carried out.

The Law of Negligence

The Law of Negligence has certain essential attributes which indisputably fall on the shoulders of educators and the organisational structure above and behind them. It is an important Doctrine of Law that operates very strongly between Academy and Pupil.

The Duty of Care that arises on Teacher, Headteacher, Governor, Academy Trust and ICT Risk Manager cannot be 'delegated away'. It cannot be avoided. it cannot be ignored. To operate in circumstances of ignorance of the law or wilful blindness to it affords no defence to it whatsoever.

The toxicity of parts of the Internet to young and developing minds, the interest of children in inappropriate risk taking and the susceptibility of Academy ICT to be used as a vector of hostility and bullying are now unarguable given facts.

> The Law of Negligence generates an e-Safety Duty of Care on Teacher, Headteacher, Governor, Academy Trust and ICT Risk Manager cannot be 'delegated away', avoided or ignored.

Taking all of the above into account – the Academy and all of the organisations and personnel that support it must look to their Duty of Care that arises when pupils access the Academy ICT. The Duty of Care should be acknowledged, calculated and understood. Since only then can appropriate measures (whether procedural, structural or Active Supervision Technologies) be introduced so that this inescapable duty is fulfilled.

The application of the Law of Negligence to Student e-Safety is addressed in two Smoothwall White Papers I have prepared.

The Doctrine of Allurements

Perhaps the most important case that most clearly sets down the duty owed to children in respect of what the Law calls "allurements" and "traps" is where the House of Lords (the then highest Court of Appeal in the United Kingdom) dealt with the case of a young boy who suffered spinal injuries when playing on an abandoned and derelict boat.

The case is as much discussed as an Occupier Liability Law case – but is wholly applicable to the exposure of students, by their Academy, to the Internet and E-Mail. It is a 2000 case called A.P. Jolley v. Sutton London Borough Council.

> The Rule of Law is that the Academy need not foresee the precise harm caused by a pupil's exposure to Inappropriate Internet Material or Malicious Messaging.
>
> Nor does not matter that the pupil suffered consequences of unexpected severity from their encounter with Toxic Content or Messaging.

The Law Says:

"*...it has been repeatedly said in cases about children that their ingenuity in finding unexpected ways of doing mischief to themselves and others should never be underestimated.*"

Let us paraphrase that statement into the 21st Century world of Academy provided Internet access, e-mail accounts and other forms of e-messaging:

"I think that the judge's broad description of the risk as being that children would "*meddle with the School's ICT at the risk of some significant exposure to extreme material and further meddle with it to bully and harass each other*" was the correct one to adopt on the facts of this case."

Now, without wishing to be repetitive, the matter that the Law recognises that "*...it has been repeatedly said in cases about children that their ingenuity in finding unexpected ways of doing mischief to themselves and others should never be underestimated.*" is similarly reflected in the daily experiences of those professionals who are responsible for the design, operation and maintenance of a School's IT Infrastructure.

Here is a statement on the subject from such a person[2]:

"*The implementation of ICT in any School or College produces tensions (such as the Need To Educate vs. e-Safety and School Legal Exposure) that combine to impact these institutions in ways that I believe are unique. For example, no other organisation, of which I am aware, is required to allow 80% of its network users to be people with characteristics which include (some or all of):- inquisitiveness, hunger for new experience, extreme competitiveness, boundless imagination, rebelliousness and self-obsession. A user group which is not only extraordinarily technology-savvy; but expert in self-justification and regularly hormone-driven.*"

The presence of an Allurement decreases the threshold of liability for the School which means that the School is obliged, in Law, to take every reasonable step to prevent Students for seeing inappropriate material and undertaking inappropriate (and harmful) e-behaviour. The School will have to take into account other factors in deciding whether a given probability of injury generates a duty – whether avoiding the risk would involve undue cost or require abstaining from some otherwise reasonable activity.

It is here that the development in the 21st Century of Active Supervision Technologies come into play. A School's consideration of them is a given – since, in my opinion, the given probability of injury when a child is in contact with toxic material is high; and the avoidance of such risk neither involves undue cost or require the School's abstinence from some otherwise reasonable activity.

The Law of Occupiers Liability

Unlike the School – the Academy owns the land and the buildings upon which it carries out its activities. Even with respect to e-Safety, the Occupiers Liability Act 1984 operates In this instance to provide an initial entrée to this matter, I will knit different parts of a Legal Judgement concerning the injury of two boys on council land to give clarity to this complex legal issue.

"The issue in this appeal is a very narrow one. The council admits that it was the occupier of the grassed area near the flats where the plaintiff lived, that plaintiff was allowed to play there and that he was accordingly a "visitor" upon its land[3] within the meaning of the Occupiers' Liability Act 1957: see section 1(2). The council therefore owed the plaintiff the "common duty of care" defined in section 2(2) of the Act:[4]

The Occupier Liability Acts require, as a matter of Law, Academies to take care to keep their pupils reasonably safe.

In addition, the Occupier Liability Acts require, as a matter of Law, – Academies to recognise and be prepared for the fact that Children are Less Careful Than Adults.

2 Mr. Dave Tonnison, a College Director of ICT Strategy with 28 years of IT experience (20 with IT vendors), paraphrasing his own previous comment in a Discussion in the "e-Safety in Education Group" on LinkedIn.

3 Pupils of an Academy are similarly "visitors" under this act.

4 Academies owe their Pupils this "common duty of care".

"…*a duty to take such care as in all the circumstances of the case is reasonable to see that the visitor will be reasonably safe in using the premises for the purposes for which he is invited or permitted by the occupier to be there*."

By way of further explanation, section 1(3) says that the relevant circumstances will include:

"...*the degree of care, and want of care, which would ordinarily be looked for in such a visitor*" so that, for example, in proper cases: "…*an occupier must be prepared for children to be less careful than adults*…"

It is also agreed that the plaintiff must show that the injury which he suffered fell within the scope of the council's duty and that in cases of physical injury, the scope of the duty is determined by whether or not the injury fell within a description which could be said to have been reasonably foreseeable – a term explained in the Negligence White Papers.

Particular attention will need to be given then, to this form of Statutory Liability which – for most Schools before they were Academies – did not exist.

Data Protection Law

The action of the Data Protection Act 1998 is one of the most pervasive pieces of legislation with respect to all of the corporate world – into which Academies have now been introduced. In this section, I will be seeking to introduce some of the core elements of the Data Protection Act 1998.

It is, in my opinion, absolutely critical for the Academy to assess and (where possible) use technology – chiefly because the Act itself tells us that "... *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data*."

The escape of Pupil Personal Data (which will include Photographs) can expose the Academy to a fine of up to £500,000.

One has got bear at the forefront of one's mind that this is a legal or law-based discussion. As the Act regulates the use of "*personal data*" it is necessary to understand what personal data means, which means that we need to first look at how the Act defines the word "data".

It must also be borne in mind by the Academy that a breach of the Data Protection Act which causes the release of Student Personal Private Data – may also be a breach of Court Order in respect of the Child in question – which will generate an additional tier of Legal Liability.

Schedule 1 to the Data Protection Act 1998 lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Copyright Information