Digital Rights and Responsibilities Guide (defamation, privacy and access)

Peter Kirwan and Tracey Binnie
Haddington Citizens Advice Bureau

The Digital Access Project, to employ staff to provide training in digital access to address poverty and increase wellbeing, was funded in part with a grant from the Scottish Government and the European Community Tyne Esk LEADER 2014-2020 Programme

Contents

Introduction to the Guide

The definition of digital rights and responsibilities is largely defined as having the right and freedom to access all forms of digital technology, with the right to privacy and freedom of personal expression with the expectation of behaving in an acceptable and appropriate manner.

This guide is intended to be used for quick reference and covers the main aspects of digital rights and responsibilities. The legal focus is primarily on Scottish law, extending to UK law on legislation reserved to Westminster. The Further Reading section at the end of the guide contains useful links covering the topics discussed.

Communication - What you can and can't say online

Introduction to online communication

The internet is interactive in a way that radio, television or newspapers never were. While you could submit to the newspapers' "letters" section or phone in to TV and radio shows, the bulk of the content was created for you not by you. Online, however, many of us are creating the content. Often this means contributing to existing conversations but sometimes it means starting them. While there are other places online we can contribute, usually this will be on social media.

When there's so much opportunity for speech, it's important to look at our rights and responsibilities around these conversations. Just as when we talk in a pub or cafe, write to a local paper or call a radio phone in, our words have consequences online and, depending on what we say, these can include legal consequences.

There is, however, a common misconception that things said online are less serious and carry lower consequences than the same things said "in real life". This mistaken view of the law, coupled with the ability to say things while apparently anonymous, leads many to say things that they simply wouldn't in person. This has led to the rise of "trolling" where people post insulting messages online (usually on social media) in order to provoke reactions from other people. Trolling is, sadly, widespread with 5 internet trolls arrested a day in 2016[1]

The contrast between these attitudes and the weight given to online offences by

[1] https://www.telegraph.co.uk/news/uknews/law-and-order/11627180/Five-internet-trolls-a-day-convicted-in-UK-as-figures-show-ten-fold-increase.html

the law is stark with Lord Advocate Frank Mulholland QC, of the Crown Office and Procurator Fiscal Service (COPFS), saying that:

"The rule of thumb is simple - if it would be illegal to say it on the street, it is illegal to say it online."[2]

The Crown Office and Procurator Fiscal Service (COPFS) also states clearly that

"we take these [communications] offences as seriously as crimes committed in person"[3]

Let's take a closer look at the legal rules around what we can and can't say in four areas: defamation, general threats, hate crimes and incitement or stirring up offences.

Defamation

The law is changing

The current Scottish laws on defamation, which have been in effect since 1996, are under review at the time of writing.[4] Notes have been added on the likely content of forthcoming changes that may form the basis of a parliamentary bill. Exactly when these changes may take place is hard to say but they are certainly not imminent In its current form Scottish defamation law is quite different from the English and Welsh[5] system which was updated in 2013.

What is defamation?

When false and unsubstantiated rumours are shared about someone, it can seriously impact their reputation and, therefore, their life and work. For this reason we have laws about "defamation" which has been defined by the Scottish Government as

[2] http://www.copfs.gov.uk/media-site/latest-news-from-copfs/926-crown-office-sets-out-social-media-prosecution-policy

[3] http://www.copfs.gov.uk/media-site/latest-news-from-copfs/926-crown-office-sets-out-social-media-prosecution-policy

[4] https://www.gov.scot/publications/defamation-scots-law-consultation/

[5] An excellent comparison of the differences can be found at Brodies https://brodies.com/binformed/legal-updates/defamation-differences-between-scotland-and-england

"the delict (i.e. wrongdoing) of defamation [that] occurs when a person makes a communication which contains a damaging and untrue imputation against the reputation of another person."[6]

In many other countries defamation is split into libel (written defamation) and slander (spoken defamation) but in Scots law these are both just referred to as defamation. Defamation falls under civil, as opposed to criminal, law which means those losing a defamation case will normally pay an amount of money to the party who won as compensation.

Defamation online: The significance of retweets and shares

While most people have heard of these laws, many don't know that they apply equally online with 46% of 18- to 24-year-olds in the UK, for example, unaware that they can be sued for sharing an unsubstantiated rumour about someone[7]

Defamation applies not just to what we post online but also what we reshare. Simply resharing someone else's defamatory social media post or website page may constitute defamation as this can be seen as an endorsement of the original statement. Some Twitter users include the warning on their profile that "retweets do not indicate endorsement" but disclaimers have to date not been shown to carry legal weight.[8] In Scots law each time the statement is published there is a new chance to bring a defamation case and each reshare/retweet on social media is seen as a separate act of publishing.

While the Defamation Act (Scotland) 1996 limits publishers to "commercial publisher, that is, a person whose business is issuing material to the public", it is not enough to show one is not a publisher, author or editor. One must also show that they "took reasonable care in relation to its publication" and that they "did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement". In short, then, one can acquire part of the responsibility for publishing a defamatory statement even though one is not the publisher, author or editor.[9] This is in contrast to English and Welsh law which has a "single publication rule"[10] though Scottish law may change to come into line with England and Wales on the issue. This current multiple publication rule in Scotland also means that the deleting of a social media post does not entirely

---

6 https://www2.gov.scot/Publications/2011/01/11092246/4

7 https://www.theguardian.com/law/2016/aug/12/social-media-law-an-essential-guide

8 It is worth noting that there is ongoing debate about the status of retweets. See https://www.linkedin.com/pulse/libel-retweeting-harry-small/ for example.

9 https://www.legislation.gov.uk/ukpga/1996/31

10 https://www.thompsons-scotland.co.uk/blog/29-employment-law/2905-defamation-law-in-the-social-media-age

protect against a defamation case because the content may continue to exist in the reshares of others.

Defence against defamation charges

To balance the protection of reputation with freedom of expression, there are several valid defences against a charge of defamation. These do not include claiming that an alleged act of defamation was unintentional. Valid defences include "truth", "public interest" and "fair comment." The truth defence is simply the principle that true statements can't qualify as defamation. The public interest defence (discussed later in forthcoming changes) requires that the defender can show that their publishing of the content was both "responsible" and in the public interest. "Fair comment" (also called "honest opinion") is when the statement in question is an "honestly held comment or opinion based on a matter of fact" as opposed to a "statement of fact" alone.[11] Unlike "statements of fact," "comments" and "opinions" can't be proved true or false. So "Andy Murray was born in 1990" is a statement of fact because it can be shown to be true or false. By contrast, "Andy Murray has a beautiful serve" is a comment because, while people may agree or disagree, there is no way to prove it true or false.

In the recent case of Stuart Campbell vs Kezia Dugdale this defence was successfully used by Dugdale. Before getting into the specifics of Dugdale's defence, some context on the case will be helpful.
Stuart Campbell, who posts on Twitter as "Wings Over Scotland," posted the following tweet:

> "Oliver Mundell is the sort of public speaker that makes you wish his dad had embraced his homosexuality sooner".

Dugdale wrote, in her national newspaper column, that she considered this tweet homophobic. Campbell not only denied the tweet was homophobic but stated that the suggestion he was himself homophobic was both false and very damaging to his career. He then sued for defamation, asking for £25,000 in damages.[12]

The case went to court where the judge found in Dugdale's favour on the grounds of "fair comment". In order for Dugdale to win it was not enough for her comment to be seen by the judge as "comment" rather than "statement of fact". For her comment to qualify as a "**fair** comment" it needed to also meet three other criteria.

---

[11] The exact definition given by the Inner House of the Court of Service is ""[t]he expression of an opinion as to a state of facts truly set forth [which] is not actionable, even when that opinion is couched in vituperative or contumelious language."" Massie v McCaig, 2013, SC343

[12] https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2018scedin49.pdf

- First, the facts upon which the comment was based needed to be stated or easily accessible to readers so they could make up their own minds.
- Second, the facts upon which the comment was based needed to be true. In this case the facts were uncontroversial because no one disputed the existence of the tweet. Had Dugdale said she found Campbell's tweet homphobic when no tweet existed, then this requirement would not have been met.
- Third and finally, Dugdale's legal team had to demonstrate that her comment was in the public interest.[13]

Avoiding court proceedings with an offer of amends

While not a defence, the Defamation Act of 1996[14] gives the defender the option to avoid court proceedings by admitting fault and making an "offer of amends." This offer of amends must take the form of an apology or retraction, include the payment of damages and must be offered before a defence is lodged. If this offer is accepted, then the person claiming defamation cannot start or continue court proceedings except to enforce the giving of amends. There is no time limit on when this offer can be accepted or rejected.

Possible changes to defamation law in Scotland

At the time of writing, Scottish law on defamation is due to undergo reform. Having reviewed the existing laws, the Scottish Law Commission (SLC) recommended a number of specific changes.[15] These would all directly impact cases where the alleged defamation has occurred online. At the time of writing a bill has yet to be laid before parliament.

To protect those criticising powerful interests, the SLC is suggesting that any defamation charges first meet a "serious harm" requirement before being brought before court.[16] If passed, a statement would not be considered defamatory unless it has caused or is likely to cause serious harm to a person or organisation.

---

[13] For a listing of these requirements see https://www.gov.scot/publications/defamation-scots-law-consultation/pages/6/ while for an interpretation of how they apply to this case by Media Lawyer David McKie see his interview with STV here https://stv.tv/news/scotland/1437124-confused-by-fair-comment-in-defamation-cases/

[14] https://www.gov.scot/publications/defamation-scots-law-consultation/pages/7/

[15] All recommended changes are detailed here https://www.scotlawcom.gov.uk/files/7315/1316/5353/Report_on_Defamation_Report_No_248.pdf

[16] https://www.scotlawcom.gov.uk/files/7315/1316/5353/Report_on_Defamation_Report_No_248.pdf section 2.9

Organisations would not be considered to have suffered serious harm to their reputation unless it could be shown that they have suffered serious financial losses.[17] This would bring Scottish law into line with England and Wales who already have such a requirement.[18] This change would have a major impact on many cases and it is notable that lawyers for Kezia Dugdale claim that a serious harm requirement would have stopped Dugdale v Campbell from ever going to a courtroom.[19] This proposed change is, however, not inevitable as it has been contested by other groups including The Faculty of Advocates.[20]

In another move to protect those criticising powerful interests, the SLC is proposing that a public interest defence against defamation, currently recognised only through legal precedent, be written into law.[21] Broadly speaking, this would mean that something is not considered defamation if it can be shown that it was reasonable for the defender to believe that publication was in the public interest.

To make the law more relevant to the current social media age, the SLC has also recommended a single publication rule and a reduction in limitation.[22] Limitation is how long someone has to bring a defamation case and in Scotland this is currently set at three years from them becoming aware of the content. Currently Scotland has what's called a multiple publication rule which means that this three year clock starts again with each republication of the original content. As discussed earlier, retweets and shares can potentially be considered new publications. Moving to a single publication rule and reducing the limitation to one year, as the SLC recommends, means that pursuers would have one year from becoming aware of the content in which to bring a defamation claim and that this clock would not be reset upon republication in the form of retweets, shares or any other form.

The reason for this change is that social media generally ensures that, if a reputation is going to be seriously harmed by content, this will happen well within a year. In this way Scotland would come more into line with the law in England and Wales which has already brought in a single publication rule and has a

---

17 https://www.scotlawcom.gov.uk/files/5715/0123/0435/Defamation_and_Malicious_Publications_Scotland_Bill_-_consultation_draft_-_Bill.pdf

18 https://www.legislation.gov.uk/ukpga/2013/26/crossheading/requirement-of-serious-harm

19 https://www.scottishlegal.com/article/faculty-reiterates-opposition-to-serious-harm-test-for-scottish-defamation-actions

20 http://www.advocates.org.uk/news-and-responses/news/2019/apr/no-serious-harm-test-in-defamation-says-faculty

21 http://www.scotlawcom.gov.uk/files/5114/5820/6101/Discussion_Paper_on_Defamation_DP_No_161.pdf section 6.15

22 http://www.scotlawcom.gov.uk/files/5114/5820/6101/Discussion_Paper_on_Defamation_DP_No_161.pdf section 10.2

limitation period of one year which starts not on the pursuer becoming aware of the content but from the content being first published. In Scotland, the courts are allowed, in special cases, to use their discretion to override the limitation period and let pursuers bring defamation cases even when the limitation clock has run out.

Finally, another area that the SLC are to change is how responsible internet companies (e.g. Twitter, Facebook, Google etc.) are for the things published on their platforms. Prior to the internet if someone put an allegedly defamatory advertisement in a newspaper, then not only the person but also the newspaper could potentially be found guilty of defamation.

At the time of writing there has, the SLC say, "been little in the way of Scottish case law on the responsibility of internet intermediaries [i.e. companies]". In law there are two recognised defences available to internet companies. One based on section 1 of the Defamation Act 1996 and the other based on regulations 17 to 19 of the Electronic Commerce (EC Directive) Regulations 2002. In order to use the 1996 Act as a defence the internet company would have to demonstrate that they are not responsible for the publication of the content or specifically:

"i. that they are not the author, editor or publisher of the statement complained of;
ii. that they took reasonable care in relation to its publication; **and**
iii. that they did not know, and had no reason to believe, that they caused or contributed to the publication of a defamatory statement."[23]

The exact details of the three defences based on the 2002 Act are quite complex but require the internet company to show, amongst other things, that they delivered but did not create the content in question. The Act provides different levels of protection for companies depending on which of three classifications they fall into. These classifications are about how much involvement the company had in the delivery, storage and any changes made to the content in question.

The 2002 Act is limited to internet services for which payment is taken and so many online services (Facebook, Twitter, Google) which are free for most users may not be able to use it. This is very much a grey area as the SLC say

"It is not free from doubt whether or not search engines are such a provider given that they are not normally paid for their services by the user but through advertisements"[24]

---

[23] https://www.gov.scot/publications/defamation-scots-law-consultation/pages/5/ section 98

[24] http://www.scotlawcom.gov.uk/files/5114/5820/6101/Discussion_Paper_on_Defamation_DP_No_161.pdf section 7.14

As the SLC say, the law in this area is quite unclear and they are unsure how exactly it should be reformed. Until a more in depth review can be carried out on internet company liability, the SLC have recommended an interim solution. This interim solution is to hold that defamation charges cannot be brought against someone unless they are the author, editor or publisher of the content in question or an employee/agent of them.[25] This would apply to internet companies as well as some other entities.

Hate Crimes and General Threats

General Threats and menacing

None of us have the right to threaten or intimidate other people online and doing so may be considered an offence, specifically ""improper use of a public electronic communications network" by threats or menacing behaviour under section 127 of the Communications Act 2003.[26] There have been a number of convictions under this part of the act. One very illustrative case is that of Peter Nunn who was jailed for 18 weeks for six abusive tweets about and to the Labour MP Stella Creasy. It's important to note that some of these tweets were not originally written by Nunn but were retweets of original tweets by other people threatening to rape the victim.[27] As in defamation cases, a person can potentially be held as liable for these as they would be if they had published the social media post themselves.

Online Hate Crime

Threats and menacing behaviour online can, in some cases, also qualify as a hate crime. Before looking at these specifically, let's first take a step back and look at Scottish laws on hate crime in general. Partly because hate crime references such a wide range of social groups, the current law on the subject is the result of many different laws.[28]

The definition of Hate Crime given by Police Scotland is a good place to start which is

[25] https://www.gov.scot/publications/defamation-scots-law-consultation/pages/5/ section 104

[26] This is an act of the UK parliament that applies to Scotland

[27] https://www.theguardian.com/uk-news/2014/sep/29/peter-nunn-jailed-abusive-tweets-mp-stella-creasy

[28] A detailed citation and explanation of all current hate crime laws in Scotland can be found in Appendix 3 of https://www.gov.scot/publications/independent-review-hate-crime-legislation-scotland-final-report/pages/14/

"Crime motivated by malice or ill will towards a social group by: race,[29] sexual orientation, religion/faith, disability, transgender/gender identity."[30]

It's important to note that, at the time of writing, this list of protected characteristics does not include age, gender[31] or membership of a subculture. The exclusion of these three groups and others is a matter of ongoing debate and controversy.

Hate crime is then a broad category where anything that would normally qualify as a crime can also be a hate crime if motivated by "malice or ill will" towards these protected groups. If someone deliberately breaks the windows of your house that's criminal damage but, if the crime has the required motives, then it also counts as a hate crime. Similarly, any sort of physical assault is a crime but it becomes a hate crime if it has the specified motivations. Hate crime is, in these cases, an "aggravation" that makes the underlying offence more serious and so carries higher penalties.

When it comes to the internet, then, hate crime applies in the same way to things that would be a crime there. In most cases of online hate crime this underlying offence is the sort of general threat offences (covered in the previous section) that arise out of section 127 of the Communications Act 2003.[32] These are online communications that are threatening or of a menacing nature. They become hate crimes when motivated by malice or ill will towards groups with protected characteristics.

Incitement and stirring up offences

While hate crimes are "statutory aggravations" that make "baseline offences" like general threats carry heavier penalties, "stirring up" hatred is a "standalone offence."[33] [34] So what exactly does "stirring up hatred" mean? Stirring up hatred is simply when someone encourages other people to hate a particular racial group. This is often referred to as the incitement of racial hatred. Unlike England and

---

[29] "Race" includes nationality, ethnicity and skin colour see https://www.hatecrimescotland.org/faq/

[30] https://www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/hate-crime/what-is-hate-crime/

[31] The reference to transgender/gender identity only refers to persons who are, or are thought to be, transgender

[32] https://www.gov.scot/publications/independent-review-hate-crime-legislation-scotland-final-report/pages/7/

[33] The Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012 did allow for stirring up offences regarding characteristics beyond race but this was repealed in 2018.

[34] These stirring up offences are a result of sections 18 to 22 of the Public Order Act 1986 which is a UK wide statute

Wales where this offence covers race, sexual orientation and religion, in Scotland the offence currently only applies to race.

For an offence to have been committed there needs to have been "threatening, abusive or insulting" conduct or material that was either intended to stir up racial hatred or, given the context, would likely have stirred up racial hatred. Unlike hate crime, here hate is important not as a motive but because it is the intended or likely effect. Importantly, the perpetrator's success in spreading hate is not required for there to have been an offence.

The UK's first conviction for incitement of racial hatred online remains a good digital example. In 2009 Simon Sheppard and Stephen Whittle were sentenced to four years and ten months and two years and four months respectively for publishing pictures online of murdered Jewish people alongside articles and cartoons mocking other racial groups.[35]

Possible legal changes

The current Scottish laws on hate crimes and related offences are under review at the time of writing. What precedes is accurate at the time of publication.[36] A comprehensive discussion of possible reform can be found at https://www.gov.scot/publications/independent-review-hate-crime-legislation-scotland-final-report/pages/4/.

The most notable of these possible changes are as follows:

- For an offence to be classed as a hate crime, the victim would not have to be a member of one of the protected groups. It would be enough that they are presumed to be a member or have some association with that group.
- Gender being added to the list of protected groups.
- Age being added to the list of protected groups.
- Stirring up/Incitement offences to cover all protected groups and not just race.
- For something to count as a stirring up offence it would be required that there have been a) threatening or abusive behaviour b) i) an intention to stir up hatred or ii) a likelihood that hatred would be stirred up.

[35] https://www.theguardian.com/world/2009/jul/10/first-racial-hatred-online-conviction

[36] https://www.gov.scot/publications/defamation-scots-law-consultation/pages/3/

Digital Rights: Privacy and Surveillance

In an ever increasing digital world, a large percentage of people's day is spent online. Whether it's to check emails, find a bus timetable, do the weekly shop or pay bills, technology and the Internet has a massive impact on our daily lives.

However, many people are unaware of how much data is actually collected on them, whether this is through a website or their device. Companies such as Facebook, Google, Pinterest etc. may offer services free at the point of use but they make their money from users by using their data as a commodity. This could be based on content, location and even by the device and operating system the user has to access sites and services.

Social media sites often claim ownership of user content. Facebook in particular is extremely intrusive by design, tracking users across the internet even if they have never owned a Facebook account.[37] If a user were to upload a photo to Facebook, for example, the company claims "a non-exclusive, transferable, sub-licensable, royalty-free and worldwide licence to host, use, distribute, modify, run, copy, publicly perform or display, translate and create derivative works of your content."[38]

Clauses like the one found in Facebook's terms and conditions are common across all social media networks, however the average user will never take the time to read them.[39] It is usually when something goes wrong that a user finds they are powerless to take action because they did not read the terms and conditions and therefore were unaware of what they were signing up for.

GDPR

The General Data Protection Regulation (GDPR) was implemented by the European Union on 25 May 2018, regulating data protection and privacy for all individuals within the European Union and European Economic Area. It also refers to the export of personal data outwith these areas, aiming to give individuals more control over their personal data and simplifying data protection regulations for international organisations dealing with the EU.[40]

Data controllers must ensure that they have appropriate technical and organisational measures in place to implement the principles detailed within the

[37] https://www.theregister.co.uk/2018/04/17/facebook_admits_to_tracking_non_users/

[38] https://www.facebook.com/terms

[39] https://www.theguardian.com/money/2011/may/11/terms-conditions-small-print-big-problems

[40] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/

legislation, using pseudonymisation or full anonymisation, where appropriate, when processing personal information. Data must not be made publicly available without explicit consent from the data subject or individual and cannot be used to identify subjects without additional information stored separately. Furthermore, a processor of a subject's personal data must clearly disclose any intended data collection and disclose the lawful basis and purpose. They must also declare how long data will be retained if shared with third parties or outwith the EU/EEA. Data subjects also have the right to request a copy of data collected and can request to have any data held erased.

Essentially, GDPR rules state that consent must be expressed consent. The data controller asks the subject for consent, explains the implications and the subject makes a genuine choice.

Data Protection Act 2018

Passed into UK law on 25 May 2018, the Data Protection Act applies the standards set by GDPR but exempts data processing that would not work in the national context, for example immigration, national security and criminal law enforcement processes.[41]

Right to erasure

Article 17 of the GDPR states that individuals have the right to have personal data erased, also known as the right to be forgotten. The underlying principle of this right is that when there is no compelling reason for their data to be processed, an individual can:

- Request a data controller to erase their personal data;
- Stop any further distribution of their personal data;
- Potentially stop third parties from processing their personal data.

Requesting erasure

If an individual decides to exercise their right to erasure, they should contact the organisation holding their data and ask for it to be erased. The individual is not obliged to give a specific reason, although they may be asked why to determine the correct conditions are met:

[41] https://ico.org.uk/for-organisations/data-protection-act-2018/

- The data is no longer necessary for the purpose for which it was originally collected or processed for;
- The data controller relies on consent as its lawful basis for holding the data and the individual withdraws their consent;
- The individual objects to the processing of their data and there is no overriding legitimate interest to continue;
- Personal data is being used for direct marketing purposes and the individual objects to this;
- Personal data has been used unlawfully, i.e. in breach of the lawfulness requirement of the 1st principle;
- Compliance with a legal obligation; or
- Personal data has been processed to offer information society services to a child.

The request can either be verbal or in writing. It is recommended, however, that any verbal requests are followed up in writing to provide clear proof of the individual's actions should there be any subsequent challenges.[42]

The right to erasure is not absolute, however, and only applies in certain circumstances such as:

- Personal data is no longer necessary for the purpose for which it was originally collected or processed for;
- The individual has withdrawn consent for holding data;
- The individual objects to the processing of their data even if the data controller is using it for legitimate purposes and there is no overriding legitimate interest to continue processing;
- Personal data has been breached unlawfully;
- The data controller must comply with a legal obligation; or
- Personal data has been processed to offer information society services to a child.

There is an emphasis on the right to erasure if the request relates to data collected from children, reflecting their enhanced protection, especially online.

If personal data has been disclosed to third parties by the data controller, they must contact each recipient and inform them of the erasure request, unless impossible or involves disproportionate effort. They must also contact the individual about any third party recipients. A recipient is defined as a natural or

[42] https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/

legal person, public authority, agency or any other body to which personal data has been disclosed, which also includes controllers, processors and individuals who are authorised to process personal data under the direct authority of the data controller or processor.

If personal data has been made public online, reasonable steps should be taken by the data controller to inform other controllers to erase links to, copies or replication to the data.

Exemptions

The right to erasure does not apply if processing is necessary for the following reasons:

- To exercise the right of freedom of expression and information;
- Compliance with a legal obligation;
- Performing a task to be carried out in the public interest or exercise of official authority;
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- For the establishment, exercise or defence of legal claims.

There are two circumstances where the right to erasure does not apply to special category data:

- If data processing is necessary for health purposes in the public interest, e.g. protecting against serious cross border health threats or ensuring high standards of quality and safety of health care and medicinal products or devices; or
- If data processing is necessary for the purposes of preventive or occupational medicine. This only applies where data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy, e.g. a health professional.

Subject Access Requests

A subject access request (SAR) is a written request to an organisation asking for access to the personal information it holds on individuals. This is a legal right in the UK and is free of charge since the introduction of GDPR legislation.[43]

In addition to allowing individuals to view the personal data an organisation holds on them, this right also allows the requester to verify that their data is being processed lawfully.

If a SAR is made to an organisation, they are legally obliged by the Data Protection Act 2018 to respond within a month, starting from the day they receive the request. An organisation may extend this period by a further two months if the request is complex or numerous, but must inform the individual within the initial one month timeframe with an explanation as to why the extension is necessary. If a request is deemed to be excessive, in particular if it is repetitive, the organisation can charge a reasonable fee. A charge can also be applied to a request for multiple copies of the same information.

Organisations reserve the right to withhold certain information from an individual, for example:

- If the information identifies another individual
- If the requester is being investigated for a crime or in connection with taxes and the investigation would be prejudiced if the requester had access to that information

Freedom of Information Act

The Freedom of Information (Scotland) Act 2002 gives all individuals the right to access recorded information held by most Scottish public sector organisations. For UK organisations, the Freedom of Information Act 2000 applies. Some organisations, such as the Ministry of Defence, are exempt. A full list of organisations that individuals can make requests to can be found on the UK government's site; the following list provides a high level overview:

- Government departments
- Public bodies and committees
- Local councils
- Schools, colleges and universities

[43] https://www.which.co.uk/consumer-rights/advice/how-do-i-make-a-subject-access-request

- Health trusts, hospitals and GP surgeries
- Publicly owned companies
- Publicly funded museums

Ensuring compliance

All organisations that process personal information are legally required to register with the Information Commissioner's Office (ICO). The ICO is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals, with offices in all four home nations of the UK.[44] It is responsible for regulating the Data Protection Act and enforcing penalties on organisations that do not comply.

[44] https://ico.org.uk/about-the-ico/who-we-are/

Digital Access Rights

The right to Internet access

In 2011 a United Nations report declared that Internet access should be a human right; it also stated that disconnecting or denying Internet access is a human rights violation and against international law. The report subsequently gained support from a wide audience of governments and industry leaders.[45]

The UK Government plans to introduce a Universal Service Obligation (USO), giving everyone the legal right to request a minimum broadband connection speed of 10Mbps, to 100% of households by 2020, raising the current minimum of 2Mbps significantly. This places access to fast broadband on a par with other essential utilities such as gas, electricity and water.

While the Scottish Government recommends a USO of 30Mbps to keep in line with superfast broadband speeds (defined as being a speed of at least 24Mbps), defining a broadband USO for the UK as a whole is reserved to the Westminster government. However, in conjunction with the Scottish Government's R100 (Reaching 100) programme, the £600m Digital Scotland's Superfast For All project successfully delivered the Scottish Government's USO to 95% of Scottish households at the end of 2017 with a target of 100% coverage by 2021.[46] There have been some challenges in delivering 100% coverage owing to Scotland's geography, some coverage is being delivered by a wide variety of infrastructure solutions including 4G, fixed wireless and emerging technologies such as TV White Space.

For households and businesses yet to benefit from the rollout, the Better Broadband scheme is a UK wide interim solution consisting of a voucher scheme to subsidise hardware, installation and connection costs to ensure first year costs are no more than £400.[47] Premises that have a download speed of less than 2Mbps and will not benefit from the R100 rollout within the next 12 months are eligible.

[45] https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[46] https://www.gov.scot/publications/reaching-100-superfast-broadband/pages/0/
[47] https://basicbroadband.culture.gov.uk/home/background/

Further Reading

For more detailed information on the subjects covered in this guide, please use the links in this section.

Further reading on defamation online laws

Crown Office and Procurator Fiscal Service (COPFS) policy guidance on communications sent via social media
https://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Book_of_Regulations/Final%20version%2026%2011%2014.pdf

Justice Directorate's 2019 Consultation Paper on Defamation in Scots Law
https://www.gov.scot/publications/defamation-scots-law-consultation/

Scottish Law Commission's 2017 Report on Defamation
https://www.scotlawcom.gov.uk/files/7315/1316/5353/Report_on_Defamation_Report_No_248.pdf

Defamation: Differences between Scotland and England by Brodies
https://brodies.com/binformed/legal-updates/defamation-differences-between-scotland-and-england

Defamation in the social media age by Thompsons
https://www.thompsons-scotland.co.uk/blog/29-employment-law/2905-defamation-law-in-the-social-media-age

Judgement of Sheriff Kenneth J McGowan in the cause of Stuart Campbell against Kezia Dugdale
https://www.scotcourts.gov.uk/docs/default-source/cos-general-docs/pdf-docs-for-opinions/2018scedin49.pdf

Defamation and Malicious Publications (Scotland) Bill (Consultation Draft)
https://www.scotlawcom.gov.uk/files/5715/0123/0435/Defamation_and_Malicious_Publications_Scotland_Bill_-_consultation_draft_-_Bill.pdf

Scottish Law Commission's 2016 Discussion Paper on Defamation
http://www.scotlawcom.gov.uk/files/5114/5820/6101/Discussion_Paper_on_Defamation_DP_No_161.pdf

Further reading on general threats, hate crime and stirring up/incitement offences

Justice Directorate's 2018 Independent review of hate crime legislation in Scotland: final report
https://www.gov.scot/publications/independent-review-hate-crime-legislation-scotland-final-report/

A useful FAQ on hatecrime by Hate Crime Scotland
https://www.hatecrimescotland.org/faq/

Police Scotland guide to hate crime https://www.scotland.police.uk/keep-safe/advice-for-victims-of-crime/hate-crime/what-is-hate-crime/

Privacy

ICO - Guide to the General Data Protection Regulation (GDPR) for organisations
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

ICO - Guide to the General Data Protection Regulation (GDPR) for individuals
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

ICO - Data Protection Act 2018
https://ico.org.uk/for-organisations/data-protection-act-2018/

Digital Access Rights

Digital Scotland Superfast Broadband
https://www.scotlandsuperfast.com/

Scottish Government - Reaching 100%: superfast broadband for all
https://www.gov.scot/publications/reaching-100-superfast-broadband/pages/0/

UK Government - Better Broadband
https://basicbroadband.culture.gov.uk/home/background/