Grŵp yr Ysgrifennydd Parhaol
Permanent Secretary's Group

Llywodraeth Cymru
Welsh Government

Our ref: ATISN 12791
Date: 19 December 2018

Dear ,

Request for information reference ATISN 12791

Thank you for your request which I received on 21 November 2018 . You asked for:

Copies of guidance to staff on how to deal with vexatious complainers or correspondence.

The information you requested is enclosed at annexe 1 to this letter.

If you are dissatisfied with the Welsh Government's handling of your request, you can ask for an internal review within 40 working days of the date of this response. Requests for an internal review should be addressed to the Welsh Government's Freedom of Information Officer at:

Information Rights Unit,
Welsh Government,
Cathays Park,
Cardiff,
CF10 3NQ

or Email: Freedom.ofinformation@gov.wales

Please remember to quote the ATISN reference number above.

You also have the right to complain to the Information Commissioner. The Information Commissioner can be contacted at: Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.

However, please note that the Commissioner will not normally investigate a complaint until it has been through our own internal review process.

Yours sincerely

Annexe 1

PEOPLE POLICIES AND PROCEDURES

GUIDANCE NOTE

DEALING WITH UNACCEPTABLE CUSTOMER BEHAVIOUR

1. Introduction

1.1 We expect our staff to be treated with courtesy and respect and violent or abusive behaviour will not be tolerated towards Welsh Government staff. Our customers rarely cause problems on the scale faced by some public sector bodies but we cannot afford to be complacent. Even a small incident can escalate if not carefully handled. On occasion, due to the highly emotive nature of the work carried out by some staff e.g. CAFCASS Cymru, these staff may be subjected to unacceptable behaviours including threats by customers and service users.

1.2 This Guidance sets out the course of action to follow if staff experience unacceptable customer behaviour and the associated roles and responsibilities. It should be read in conjunction with the Managing Unacceptable Communications Guidance.

2. Prevention is better than cure

2.1 Annex 2 lists some general preventative measures which all staff must take when dealing with customers by telephone, correspondence or face to face. Managers must ensure that these measures are brought to the attention of all staff especially those who are new to the Welsh Government.

.

3. What is unacceptable behaviour?

3.1 The Health and Safety Executive (HSE) define violence at work as: "any incident in which an employee is abused, threatened, or assaulted by a member of the public in circumstances arising out of the course of his or her employment".

3.2 Apart from actual physical assault, violence or the threat of violence may include:

- severe verbal abuse
- words or actions likely to result in actual violence
- serious or persistent harassment
- racial or sexual harassment
- damage or threats of damage to personal/official property

- or the above may be directed against an employee's immediate family because of their work.

4. What you must do if you experience unacceptable behaviour

4.1 The Welsh Government regards any incident of violent and abusive nature directed against its staff as serious and we will take action in accordance with this Guidance to protect staff. The first consideration is for the safety and well being of staff. You must therefore:

- **always** consult your line manager if you have any concerns in relation to your personal safety;
- **never** take unnecessary risks in matters which may affect your personal safety or the safety of others; and,
- **always** withdraw from any situation if there is the threat of violence.

4.2 If you have any concerns about visitors or potential visitors then make these concerns known to your line manager and to reception and/or security staff depending on your location.

4.3 Your line manager needs to know the exact circumstances of your concern so that, for example, the case for additional security guards or a police presence can be considered**. If you are subjected to any of the behaviours indicated in paragraph 3 you must <u>always</u> report it to at least your line manager and possibly FCS Departmental Security Unit and/or the police depending on the nature of the incident.** For advice on reporting and maintaining records of incidents see paragraph 15 below.

5. Management responsibilities

5.1 All managers have responsibility for the safety of their staff. Involvement in the handling of a violent or abusive incident is a vital part of the role of managers at all levels and may help to prevent a repetition of such problems.

5.2 Where a customer has clearly behaved unacceptably to a member of staff, a manager (Management Band 2 and above) should, where practicable, talk to the customer to try to find out what has caused them to behave in an unacceptable manner and to reinforce the message that such behaviour will not be tolerated. This may be immediately after the incident provided that to do so does not put anyone's safety at risk. If the customer has already left the premises, the line manager is based at another Welsh Government location or it is not considered safe to discuss the incident immediately, the manager may write to the customer inviting them to meet and discuss the incident within five working days.

5.3 Such prompt action often takes the heat out of a situation and demonstrates that managers are committed to the health and safety of their staff. It should also encourage their staff to report incidents because they know that action will be taken to make the customer aware of poor behaviour and to lay down standards for the future.

5.4 When a meeting between a line manager and the customer has occurred, a report of the meeting should be followed up in writing to provide confirmation of the actions to be taken as a result, including the fact that a report of the incident has been made, what it will be used for, how long it will be retained and who it may be passed to.

5.5 However, the safety of all staff is of paramount importance and managers should never place themselves in any situation with customers that could put them at any risk of personal danger. Therefore, managers should only speak to customers in these circumstances if they are fully satisfied that it is safe to do so and that reasonable security measures are in place.

5.6 Managers, jointly with their staff, and, in consultation as necessary with FCS Departmental Security Unit, Corporate Health Team or the Trade Unions, should regularly review the adequacy of the health and safety arrangements applicable to their work. This should include evaluating:

- how likely is it that something will go wrong;
- if it does go wrong, how serious the consequences might be;
- how often the risk might arise (daily, weekly, yearly etc.);
- how many people might be affected;
- whether the effects might be immediate or longer term;
- what the effect on the business might be; and,
- what the law requires.

5.7 The risks covered should, where appropriate, include the need to protect staff from exposure to reasonably foreseeable abusive behaviour or violence. This translates into a requirement that managers at all levels review local arrangements regularly including:

- taking into account the changing circumstances of the job;
- adopting work practices which safeguard staff ;
- seeking at all times to minimise any risk factors which may affect staff safety;
- become actively involved in managing customers whose behaviour is unacceptable and develop strategies for handling particularly difficult customers on an individual basis;
- ensure the reporting of **all** unacceptable incidents; **ensure that staff receive appropriate training on managing unacceptable customer behaviour before dealing with customers either face to face or by telephone**; and,
- in serious circumstances consideration may need to be given to warning other public sector bodies. (This should be done via FCS Departmental Security Unit.)

5.8 Line managers should determine, in consultation with staff, a safe system for dealing with individual difficult customers. Options which must be considered include:

- accompanied interviews;
- use of a safe designated area which is visible to managers and colleagues;
- managers undertaking interviews;
- managers accompanying staff who are interviewing particularly difficult customers to give support and observe the customer's behaviour.

5.9 It is felt that managers are best placed to carry out these kinds of risk assessments due to their in-depth knowledge of their particular working environment but if any assistance is required, line managers should consult their senior management or FCS Departmental Security Unit, Corporate Health Team or their HR Business Partners. [See Health & Safety web page for further details]

If a member of staff is out of the office on official business and feels threatened or in danger then they should call 999 immediately for Police assistance.

6. Staff working off-site

6.1 Managers should ensure that, where a member of their team is working away from an Welsh Government office, appropriate control measures are taken. These may include issuing personal attack alarms and mobile phones. Lone workers should advise managers of the location of any external visits and their anticipated time of return. Please refer to the policy on Lone Working for further information http://assembly/healthsafety/content/hs/risk/default.htm

7. Threats involving a member of staff's home

7.1 If a customer states, suggests or implies that they know the home address of a member of staff and will carry out an assault at their home, the member of staff should immediately inform their line manager, FCS Departmental Security Unit (on 3333 or (029 2082 3333) **or e-mail Welsh Government Security (Cathays Park) welsh.security@wales.gsi.gov.uk)** and the police, stating why they believe their home address is known to the customer. The member of staff may wish to take advice on the security of their home. They can do this by contacting the police Crime Prevention Officer or FCS Departmental Security Unit who may be able to provide a trained security adviser. It is a decision solely for the member of staff as to whether to follow the advice given.

8. Reporting Procedure for Assault

8.1 Serious physical assaults should be reported to the police by the victim, their line manager or via FCS Departmental Security Unit immediately after the incident has occurred. This should be followed up in writing as soon as the member of staff is able to do so.

8.2 All assaults, attempted assaults, or threats must be reported in writing to the Line Manager who will add their comments to the report and forward it immediately to FCS Departmental Security Unit. Where necessary, some business areas may also

develop localised reporting arrangements to underpin these corporate requirements.

8.3 FCS Departmental Security Unit will acknowledge receipt of reports received and save copies in an iShare file specifically maintained for recording such incidents. The file will be made available for inspection by the Corporate Health Team, the Deputy Director, Expert Services & People FCS or the Director General of FCS when requested and by the Health & Safety Inspectorate.

8.4 Staff need to bear in mind that failure to report a first incident may prejudice subsequent action. The reporting should include all unacceptable incidents even if they are unlikely to recur since they can help management take steps targeted to where they are needed most.

8.5 Any incident report should include whenever possible, but especially in the case of a serious incident, a detailed statement from any witness and/or any first aider attending the incident. The line manager of the individual who was the subject of the incident should oversee the provision of all information relevant to the report.

8.6 As a minimum staff within the team should be advised of the incident and any remedial measures so that they can be vigilant and take measures to avoid a reoccurrence. The line manager in conjunction with FCS Departmental Security Unit should also consider whether any other staff need to be advised for safety reasons.

8.7 Incidents which may result in the person being considered to be potentially violent

8.8 Raising concerns that a person may be potentially violent is a very serious step but depending on the facts and circumstances senior management may deem it appropriate:

- if the person commits an actual physical assault on a member of staff, regardless of whether the member of staff is injured;
- if the person attempts to commit a physical assault;
- if the person makes a threat of violence either face to face or over the telephone, displays threatening or aggressive behaviour or stalks a particular member of staff;
- if the person is ***known*** *to be* suffering from a severe mental illness and they are likely to pose a danger to staff;
- on the advice of the police;
- on the advice of another organisation which has dealt with the customer.

8.9 Upon any serious incident taking place, the matter should always be referred to a senior manager (Executive Band 2 or above) who will decide on the appropriate action to take, given the nature of the incident and the particular circumstances in which it arises. Decisions on how to consider an incident must be taken on a case-by-case basis. Matters to take into consideration may include:

- reviewing any risk assessment, in consultation with the Trade Unions, FCS Departmental Security Unit and the Corporate Health Team;
- classifying the customer as potentially violent;

- ensuring that managers in other customer facing areas are advised; and,
- if need be, alerting outside organisations to any potential threat as soon as possible.

8.10 A senior manager (Executive Band 2 or above) may, where practicable, arrange to interview the customer as quickly as possible after the incident, provided always that their own personal safety is not compromised by doing so and subject to appropriate security measures being put in place and irrespective of whether the police may also want to take action themselves.

8.11 The purpose of any such interview would be to try to establish why the incident occurred. Was it because the customer was unhappy, for example, because:

- of the way they were treated?
- of long waiting times?
- they felt they were being passed from "pillar to post"?

. During the interview the manager should explain tactfully to the customer why their behaviour was unhelpful.

8.12 Following the interview the manager should also consider whether any changes should be made to Welsh Government procedures, for example, to reduce waiting times to try and prevent such a problem happening again.

8.13 The meeting may be successful in reassuring and calming the customer and reducing or removing the initial threat or potential for the unacceptable behaviour to reoccur. If the manager assesses that the potential for unacceptable behaviour remains, they must liaise with FCS Departmental Security Unit who will consider contacting the police. In the case of CAFCASS Cymru employees, the line manager may also consider contacting the local Court Service to seek further guidance on a particular case.

8.14 Members of staff involved in any incident must report it irrespective of whether they have been personally affected. Their report should go to their line manager for forwarding to FCS Departmental Security Unit. This is to ensure that details will be evaluated, appropriate safety measures introduced and other members of staff forewarned where necessary. Where the incident has been witnessed the line manager should ensure that witness reports are completed.

9. Legal Action Against an Assailant

9.1 Where the police are not called following an assault, or if they have been called and are not prepared to prosecute, then legal proceedings can be started by the person towards whom the violence was directed or by the Welsh Government if that action is considered proportionate and appropriate. It is for that person to decide whether or not to take legal action though advice can be obtained from management who may consult the Welsh Government's legal advisers.

If, after taking advice, the member of staff decides they wish to proceed, the Welsh Government will take a decision as to whether they are prepared to financially support this action. However, if the Welsh Government does not consider that a prosecution is justified and are not prepared to financially support the member of staff in taking that action, staff still have the right to start proceedings themselves without

official assistance, if they wish. In that event, the Welsh Government will not be responsible for any expenses incurred in undertaking the prosecution, nor for any costs which might be awarded against the employee.

10. Seeking legal assistance from the Welsh Government

10.1 Where an employee seeks legal assistance from the Welsh Government following an incident occurring in the course of their employment, they should put the request in writing to their line manager, who should send it to FCS Departmental Security Unit at Cathays Park together with:

- any original signed statements made personally by the individual allegedly assaulted and by any witnesses;
- a report from the line manager giving background information about the incident;
- any known details of the alleged assailant including name and current address;
- a plan or sketch (roughly to scale) of the area where the alleged assault occurred;
- any other details which might be relevant to the alleged assault;
- a photograph, where relevant, of injuries suffered.

10.2 FCS Departmental Security Unit will then take the matter up with the HR Business Partner and Legal Services. Employees should refer to the Welsh Government policy on Legal Assistance at Public Expense for further information.

11. Giving Evidence

11.1 When the Police prosecute, the individual allegedly assaulted will almost certainly be called as a witness. Normally it will not be necessary to have legal representation. However, this may be necessary where there are special circumstances, for example:

a. if there are grounds for thinking that serious allegations might be made against the individual or other staff; or

b. if disclosure of sensitive information is likely to be involved. The legal representative will have no right to speak at the hearing, but, if allegations or requests for disclosure of such information are made, the representative will discuss the action to be taken with the police prosecutor.

12 Repeated Threats, Verbal Abuse and Persistent Annoyance outside Welsh Government premises or another location at which a member of staff may be carrying out their duties

12.1 In the event of staff or their families finding that they are subjected to verbal threats and abuse, or to harassment, because they are known to work for the Welsh Government then the details should be reported to their line management who will forward the information to FCS Departmental Security Unit.

12.2 In such cases, the Welsh Government may provide legal assistance to the member of staff, to help them apply to the appropriate court for an order to stop the threats or harassment. The police may need to be called to deal with cases or threats,

especially if a threat is so menacing that the member of staff is in genuine fear of personal violence. The line manager (usually in consultation with FCS Departmental Security Unit) may discuss any apparent threat with the police without necessarily calling them to the office.

13. Sickness absence due to Assault

13.1 Sickness absence resulting from violence falls into a special category. Provided that, in the opinion of the Welsh Government, there is a good prospect of recovery and return to duty within a reasonable time period and when a member of staff has exhausted their entitlement to sickness absence at the full rate of pay, a medical assessment will be undertaken to consider whether payment of up to 85% of full pay may be granted. However, if it is considered that a return to duty is unlikely, the employee will be considered for an injury benefit award under the Principal Civil Service Pension Scheme (PCSPS). This applies even if the member of staff is a member of another pension scheme. Further details can be found in the Attendance Management policy and procedures.

14. Data Protection Act 1998

14.1 In order to comply with the Data Protection Act, any personal data in incident reports or any other personal data held by the Welsh Government about people mentioned in those reports must be:

- accurate;
- adequate, relevant and not excessive;
- not kept for longer than is necessary (see paragraph 11); and,
- only disclosed to those who have a legitimate interest in being aware of the information contained within them, including the customer who is the subject of the report.

14.2 Therefore, whilst all reports of incidents must be comprehensive, you must ensure that they are accurate, factual and non-emotive. If you are in doubt ask for assistance from a senior manager or from the Access to Information Unit.

15. Sharing and retention of incident reports

15.1 Once produced, all incident reports should be retained on a registered file within the Division concerned. Access to this file should be restricted to only those members of staff who have a legitimate reason to be aware of the information they contain. For example, if various members of a team may have contact with a customer who has been the subject of a report, it is legitimate for those individual members to be made aware of the situation (but not those who are unlikely to have contact). However, other teams within the Division who are highly unlikely to come into contact with the customer should not have access to the information in the incident report.

15.2 In certain instances, it may be necessary for other teams to have access to information about a customer. For example, if a member of staff, having had face to face contact with a customer, is receiving threatening or abusive phone calls or

e-mails, it may be necessary for switchboard staff or the Information Security team to have access to personal data such as names or e-mails addresses in order to prevent further contact. They do not need, however, to have details of the actual incident that gave rise to the abusive calls or messages.

15.3 Depending on the nature of an incident, it may be necessary for FCS Departmental Security Unit, the police and/or the Health and Safety Executive to have access to the incident report. This would be the exception rather than the rule and the team that produced the report should always query whether anyone outside the team has a legitimate interest in accessing the information.

15.4 The registered file should be weeded every six months to 12 months depending on the nature of the incident (as detailed below) to remove incident reports on individuals with whom no further contact is necessary or envisaged. The following retention periods will apply:

Nature of incident	**Retention Period**
Severe verbal abuse	6 months
Words or actions likely to result in actual violence	12 months
Serious or persistent harassment	2 years
Racial or sexual harassment	2 years
Damage or threats of damage to personal/official property	2 years
Any of the above directed against an employee's family	2 years

Annex 1

Roles and Responsibilities

Employees are responsible for:

- Making themselves aware of the guidance note;
- Ensuring that they take appropriate action if they are in receipt of unacceptable customer behaviour

Line Managers are responsible for

- Making their team aware of the guidance note and what is or is not appropriate
- Supporting their staff if they have to deal with unacceptable customer behaviour and taking initial advice from the relevant point of assistance e.g. FCS Departmental Security Unit, Health and Safety Executive via the FCS Corporate Health and/or Trade Union Side

Corporate Health team and HR Business Partners are responsible for:

- Supporting employees and managers in their understanding of the guidance note and providing further guidance on appropriate action where necessary (HR Business Partner Teams)
- Supporting those who are distressed following the experience of dealing with unacceptable customer behaviour (FCS Corporate Health Team)

FCS Departmental Security Unit are responsible for:

- Offering advice and guidance and informing the emergency services as and when necessary.

Information Security Team are responsible for:

- Providing advice on dealing with IT related communications, carrying out further investigation where possible and advising on possible preventative measures.

Annex 2

DEALING WITH UNACCEPTABLE CUSTOMER BEHAVIOUR

GENERAL PREVENTATIVES MEASURES TO BE CONSIDERED BY MANAGERS AND STAFF

Remember - a pleasant manner and a friendly approach is generally the most effective way of defusing potentially difficult situations

Do's to remember

- Treat all members of the public courteously and impartially, in a firm but friendly manner.
- Listen carefully to what customers say and make allowances for any literacy problems
- Explain things clearly and simply to avoid possible misunderstandings
- Prepare properly for interviews with customers
- Be honest and frank - if you are not sure the information you are giving is accurate, check.
- Recognise that some customers may be stressed or have physical, mental or personal problems which may influence their behaviour
- Refer to your supervisor/line manager if a customer rejects your explanation
- Always keep calm - do not allow yourself to be provoked
- Call for assistance immediately if a customer becomes aggressive and make sure you can get away quickly if necessary
- Tell your manager if you have reason to believe a customer is potentially violent

Don'ts to remember

- Don't make promises to a customer that you may not be able to keep.
- Don't give information which could be misleading
- Don't interview a customer who appears to be under the influence of drugs/alcohol, without ensuring you have colleagues nearby to assist you if required.
- Don't carry out or continue with any interview where you feel your personal safety may be in any jeopardy. Immediately report the matter to a Manager for him/her to take appropriate action.
- Don't keep a customer waiting longer than is necessary
- Don't provoke a customer through words or actions
- Don't retaliate by words or actions
- Don't try to arrest or detain an assailant

WELSH GOVERNMENT HR GUIDANCE AND PROCEDURES

MANAGING UNACCEPTABLE COMMUNICATIONS

1. Introduction

1.1 From time to time members of staff may be subject to communications from outside or within the organisation which are unacceptable because of their nature. This may be because the nature of the communication is malicious, vexatious or persistent, even after the issue raised has been addressed. Customers or service users may also make unreasonable and unacceptable demands by seeking inordinate amounts of information, by having inappropriate expectations of the nature and scale of the service they will receive or by the number of approaches they make.

1.2 What amounts to an unreasonable or unacceptable demand will depend on the circumstances surrounding the behaviour and the seriousness of the issues raised by the customer / service user and the impact they have on workload, time and resources. Examples of actions include, demanding responses within an unreasonable timescale, continual phone calls or letters, repeatedly changing the substance of a complaint or raising unrelated concerns. Such communications may be because a member of staff is dealing with a contentious policy issue, the customer / service user is unhappy with the response to the issue they have raised or the member of staff simply happened to be the person who picked up the phone. In all cases where communication is considered to be unacceptable, measures can be put in place to address the problem by other means or to cease the communication altogether.

1.3 There is no legal definition of the terms ‘malicious’ or ‘vexatious’ but they are generally understood to include communications which are offensive in tone or language, persistent to the point of constituting a nuisance, or occur because someone has an ulterior motive which is not merely the answering of the particular issue they have raised (e.g. they are ultimately seeking some form of compensation or consider they have a grievance against an individual or the organisation).

1.4 The method of communication could be by telephone, e-mail or correspondence. Whatever the method, staff in receipt of such communications can find them upsetting, frightening or frustrating. This guidance note sets out various means by which unacceptable communications can be addressed and provides information about sources of help for someone who has a particularly unpleasant or worrying experience to cope with their reaction.

1.5 Whatever form the unacceptable communication takes, it may be decided that contact or the methods of contact with the customer/service user should be restricted, provided that these restrictions do not impact on the safety of other individuals. Such a decision will be made by the deputy director. The customer/service user will be informed in writing of this decision, the nature of the restricted contact and the timescale when these arrangements will be reviewed. This decision may be reconsidered if the customer/ service user demonstrates a

more acceptable approach and requests that the decision is reviewed. The deputy director will review the case and inform the customer/service user in writing that, either the restricted contact arrangements will remain in place or a different course of action has been agreed. Relevant staff will be made aware of any restrictions in place and any case files duly noted.

1.6 In order to reduce the risk of unacceptable communications, there are actions that can be taken in advance. If a policy team knows that it is about to issue a contentious decision or a new policy which is likely to be unacceptable to a particular group or such an issue arises, the team can:

a. send out the information in an anonymised fashion so that there is no recourse to individual staff;

b. prepare briefing material, in advance wherever possible, for switchboard staff. Calls on this subject can then be dealt with by set responses from switchboard staff rather than being passed on to individual team members and switchboard staff can avoid giving the names and extension numbers of individual contacts who are dealing with the matter. Callers can also be directed by the switchboard staff to the enquiry pages on the internet rather than putting calls through to the policy team.

c. Provide copies of the briefing material to the OFMCO Departmental Security Unit and the IT Security Team so that they can be aware that unacceptable communications may arise and be prepared to put other measures into force (see below).

1.7 Staff need to bear in mind that, even if communication is unacceptable, there may be a valid Freedom of Information or Data Protection request being made within the overall message. Formal guidance on dealing with vexatious or repeated requests can be found at: Information Commissioners. The Access to Information Unit can provide you with help or advice: http://assembly/ati/contents/default.htm. Any vexatious or repeated requests will be dealt with in line with the current legislation on such issues.

2. Roles and responsibilities

2.1 Role of the Employee

- Making themselves aware of the guidance note;
- Ensuring they take appropriate action if in receipt of an unacceptable/hoax call or other unacceptable communication.

2.2 Role of the Line Manager

- Making their team aware of the guidance note and what is/is not appropriate;
- Supporting their staff if they receive an unacceptable communication and taking advice from the relevant point of assistance e.g. OFMCO Departmental Security Unit Information Security, HR Business Partner and Occupational Health, Complaints Unit or Legal Services Department if appropriate.

2.3 Role of OFMCO HR Expert Services and People Division

- Supporting employees and managers in their understanding of this guidance note and providing guidance on appropriate action where necessary (HR Business Partners).
- Providing support to those distressed following receipt of an unacceptable communication (Occupational Health).

2.4 Role of OFMCO Departmental Security Unit

- Offer advice and guidance and informing the Police when necessary.

2.5 Role of Information Security

- Providing advice on dealing with IT related communications, carrying out further investigation where possible and advising on possible preventative measures.

2.6 Role of Switchboard staff

- Receiving briefing from policy teams and making arrangements to handle unacceptable telephone calls where necessary.

3. Unacceptable telephone calls

3.1 There are relatively few telephone calls that are considered by the Welsh Government (WG) to be unacceptable. How these calls are managed depends on their nature and extent.

3.2 WG staff can be contacted directly by telephone from outside the organisation. It is impossible to screen all external calls or immediately identify the caller. It is therefore essential that staff are aware of how to manage calls that may be abusive in nature. Whilst unacceptable calls can only be traced in extreme cases and following police intervention, it is worth noting basic details about the call so that patterns can be identified and if necessary be used to track and trace an abusive call/series of calls.

3.3 Unacceptable or difficult telephone calls may be:

a. Abusive
b. Sexual/malicious
c. Hoax
d. Suicide threats
e. Bomb threats (Cathays Park) &
Bomb threats (non Cathays Park)
f. Unacceptable internal calls

a. Abusive calls

Welsh Government staff must not continue with telephone calls that are abusive or contain allegations that lack substantive evidence. This could mean that the caller is continuing to raise issues which have already been addressed or is making comments or allegations that cannot be substantiated by the information held or which is outside the responsibility of the WG. When this happens, the telephone caller should be handled as follows:

1. They must be told that their language is offensive, unnecessary and unhelpful and asked to stop otherwise the person receiving the call will end the telephone conversation immediately.

2. The threat or use of physical violence, verbal abuse or harassment towards WG staff may also result in the end of the telephone call. This will always be the case if physical violence is threatened.

3. If staff receive a call of this nature outside of normal office hours (from 7:00 am up to 8:30am or from 17:30 to 19:00) they should in the first instance report the incident to OFMCO Facilities Security Management Team on ext 3333 **or e-mail welsh.security@wales.gsi.gov.uk.** The member of staff taking the call has the right to tell the caller that the behaviour is unacceptable and end the call if the behaviour does not stop.

5. If, after terminating the call, the telephone rings again, staff should not answer it but let the call go to voicemail (staff should ensure that they have set up voicemail on their extension).

6. If it is a genuine call then the individual will be able to respond after receiving the message.

7. If a caller has left an abusive or threatening telephone message on an answer phone, it should not be deleted.

8. Incidents outlined above should be reported immediately to the line manager, a note taken containing the key characteristics of the call (using the form at Annex A) and the appropriate HR Business Partner should be consulted.

9. If the call is of a particularly abusive or threatening nature, the incident must be reported to the OFMCO Departmental Security Unit and the police.

10. Further information on dealing with such incidents can be found in the Guidance Note on Dealing with Unacceptable Customer Behaviour.

b. Sexual/Malicious calls

Calls that are sexual or malicious in nature should be treated in the same manner as those that are verbally abusive. If an employee receives such a call they should carry out the following procedure:

1. Terminate the call immediately (note any characteristics of the call as outlined in this note using the form at Annex A).

2. Staff should pay particular attention as to whether the caller addressed them by name and if so give consideration as to whether they gave this out as part of the greeting.

3. If after terminating the call the telephone rings again, do not answer it but let the call go to voicemail.

4. If it is a genuine call then they will be able to respond after receiving the message.

5. If a caller has left an abusive or threatening telephone message on an answer phone, it should not be wiped but again immediately reported to the line manager and Shared Service Help Desk (so that it can be noted in case any similar calls arise) OFMCO Departmental Security Unit and the IT Security Officer and may also be reported to the police.

c. Hoax calls

If a hoax call is received the line manager must carry out the following procedure:

1. Inform the appropriate HR Business Partner immediately.

2. Inform the Shared Service Help Desk (so that it can be noted in case any similar calls arise) and OFMCO Departmental Security Unit. The Security Team will be able to offer advice and decide whether or not the Police should be contacted.

d. Suicide Threats

In cases of suicide threats, staff should aim to keep the caller calm. If WG holds any information on the caller this may influence how the member of staff deals with the call. The recipient of the call may do some or all of the following:

a. Contact the Police/Ambulance/OFMCO Departmental Security Unit or Social Services if appropriate (possibly by passing a note discreetly to another team member whilst they continue to talk to the caller if appropriate and possible);

b. If the caller has harmed him/herself and you know their location, ask a colleague to contact the Ambulance Service;

c. Try to keep the person talking until they arrive;

d. Try to keep an accurate record of the conversation and send a copy to your line manager;

e. If the caller is in distress about a matter relating to the Department of Health and Social Services email a record of the call to the **Ateb Health enquiries external mailbox Health.enquiries@wales.gsi.gov.uk**

e. Bomb Threats for Cathays Park

If you receive a bomb warning, you should ask a colleague to immediately inform the telephone operator/security office on ext 3333 that there is a bomb warning call and on which extension number. Keep the caller in conversation for as long as possible and obtain as much information as you can. Annex A contains more details.

Bomb Threats for Non Cathays Park

Make yourself aware of any site specific instructions for bomb threats. If there are no site specific instructions and you receive a bomb warning, you should ask a colleague to immediately inform the Police by calling 999, they must inform the Police of who is calling them and address and telephone numbers. Keep the caller in conversation for as long as possible and obtain as much information as you can. Annex A contains more details.

Steps to be taken in all cases if bomb threat received

Try to ascertain:

- The exact location;
- The expected time of detonation;
- The appearance and size of the bomb;
- Who the caller is and where they are calling from;
- What type of language is being used e.g. swearing or abusive;
- Ascertain whether the caller is male or female;
- Try to determine the pattern of speech, accent;
- Whether the caller sounds intoxicated or agitated.

This information should then be passed to the Welsh Government Departmental Security Adviser as soon as the telephone call has ended.

f. Unacceptable Internal Calls

If a malicious call is made or received from within the WG then it may be defined as harassment. If you receive such a call then you should refer to the Dignity at Work policy and follow the guidance as required.

If internal calls are made anonymously, a request can be made to the Deputy Director Expert Services & People or the Director of OFMCO to allow switchboard staff to obtain records of calls to that extension **(see 5.1c below).** Those who are found to have made malicious calls internally may be subject to disciplinary proceedings.

4. Recording the Call

4.1 Whilst calls are only traced in extreme cases, making a note of the call will ensure that the key details are recorded and can be used if patterns emerge or if the Police need further details:

- Background noise, for example, outside/inside, office noise, TV/radio, conversation
- Does the call sound like it is from a landline or a mobile?
- Vocal characteristics, e.g. accent, male/female
- Do you recognise the voice?
- Date and time
- Did the caller use your name (and if so, was it used as part of your greeting or was it on the voicemail message)?
- Was the phone ring external or internal? If the call was external contact the switchboard immediately to check if they can remember whether or

not they had put a call through to your extension and if a name or number was quoted

4.2 Details of calls should be recorded on the form at Annex A.

5. Action that can be taken

5.1 If an individual has received malicious or vexatious calls, arrangements can be made for all their calls to be received via the switchboard.

a. Switchboard staff can ask the identity of the caller and advise the individual who is calling before they put the call through.

b. If the member of staff does not wish to accept the call, they can ask for a message to be taken or for calls to be put through to a central number so that they personally do not have to take the call.

c. If the caller is known to have made unacceptable calls previously or are suspected of having done so, the Deputy Director Expert Services & People or Director of OFMFO can sanction allowing switchboard staff to obtain records of calls received on a member of staff's extension number and their source.

d. The member of staff should also inform OFMCO Departmental Security Unit and the Head of Information Security.

e. In isolated and particularly serious cases and where a malicious caller is contacting a member of staff directly on their extension number, arrangements can be made for number or caller display to be provided on that extension so that the member of staff can see who is calling. Record keeping measures can also be put in place to assess the degree and frequency of contact.

NB It is not possible to prevent calls being put through from another extension, so any staff who are transferring calls should:

- take the name of the caller
- wait for the extension to be answered
- announce who the caller is and
- check that the call will be taken *before hanging up*.

5.2 If a caller is not malicious but persistent despite having received a response to their question or the issue they wished to be addressed, this can be debilitating and frustrating for staff. Staff should consider the nature of the call and seek permission to refuse to respond to the particular caller from their Deputy Director, giving details of the history of dealings with the caller. If permission is granted, the switchboard team can be informed not to let calls through from that caller to the person who has been subjected to previous unacceptable behaviour. A record should be made of the caller's attempts to contact the member of staff. This action does not preclude the caller from contacting other members of staff on other legitimate matters.

5.3 Alternatively, arrangements can be put in place by the deputy director to inform that customer/ service user that calls will only be accepted from them at set times or on

set days or that senior members of staff only deal with calls form that customer/service user.

5.4 Where records are being made of calls received to a particular extension, the retention and disposal of such records will comply with the WG Records Management (http://assembly/erecords/Records%20Management/Policy,%20Advice%20%26%20Procedures/rmpolicy.htm) and Data Protection (http://assembly/dataprotection/) policies.

6. Unacceptable e-mails

6.1 If a member of staff is receiving unacceptable e-mails, they should advise the Shared Service Help Desk (so that it can be noted in case any similar e-mails are received), OFMCO Departmental Security Unit and the IT Security Officer as indicated above. Offensive or unacceptable messages should be forwarded immediately to the IT Security mailbox.

6.2 Arrangements are already in place in the Security Policy for incoming e-mail addresses to be blocked in certain circumstances. Additional arrangements can be put in place to:

- anonymise a member of staff's e-mail address by using a generic e-mail address
- obtain records of the source of incoming e-mails
- block incoming e-mails (although this can be difficult if the person sending them changes their e-mail address)
- in extreme cases, install an outgoing message on a generic e-mail box so that all senders of incoming mail are informed that: 'if this message is offensive or criminal in nature, criminal action may be taken'.

7. Unacceptable correspondence

7.1 If staff are in receipt of malicious or vexatious correspondence and it is of a threatening or abusive nature, they should advise OFMCO Departmental Security Unit so that appropriate action can be taken.

7.2 If the correspondence is of a persistent nature, staff should seek permission to refuse to respond as indicated in **para 5.2** above, giving details of the history and nature of contact, provided they are satisfied that there is no viable Freedom of Information or Data Protection request contained within it. A record should be kept on file of the correspondence received. This action does not preclude the correspondent from writing to another member of staff about another legitimate matter.

8. Unacceptable behaviour in person

8.1 Although infrequent in most cases, there are occasions when members of the public can behave unacceptably when calling in person at a WG office or when attending a WG stand at an event. If this occurs, the Guidance Note on Dealing with Unacceptable Customer Behaviour should be followed. In the case of persistent unacceptable behaviour, the relevant HR Business Partner and OFMCO Departmental Security Unit should be informed.

8.2 If the customer/service user repeatedly visits the office, they should be required to make an appointment to see a named member of staff before visiting the office or that contact is restricted to written communication.

9. Support available

9.1 Where staff have experienced verbal abuse when answering phone calls, they may want to consider using voice mail or answer phones until they have enough confidence to accept incoming calls again.

9.2 If a member of staff is left disturbed or distressed after receiving any of unacceptable communications outlined above, they may wish to contact Occupational Health or the Employee Assistance Programme (via the intranet or on 0800 282 193) who will provide support and guidance to the individual.

10. Other useful guidance and advice

10.1 Please also refer to the Security Policy.

11. Data Protection Act 1998

11.1 In order to comply with the Data Protection Act, any personal data in records of unacceptable communication or any other personal data held by the WG about people mentioned in those reports must be:

- accurate;
- adequate, relevant and not excessive;
- not kept for longer than is necessary; and,
- only disclosed to those who have a legitimate interest in being aware of the information contained within them, including the customer who is the subject of the report.

Therefore, whilst all reports must be comprehensive, you must ensure that they are accurate, factual and non-emotive. If you are in doubt ask for assistance from a senior manager or from the Access to Information Unit.

12. Sharing and retention of records of unacceptable communications

12.1 Once produced, all records should be retained on a registered file. Access to this file should be restricted to only those members of staff who have a legitimate reason to be aware of the information they contain. For example, if various members of a team may have contact with a customer on whom a record has been produced, it is legitimate for those individual members to be made aware of the situation (but not those who are unlikely to have contact). However, other Teams within the Division who are highly unlikely to come into contact with the customer/ service user should not have access to the information at all. This may require the setting up of a caveat group on iShare to manage access to the file.

12.2 In certain instances, it may be necessary for other teams to have access to information about a customer / service user For example, if a member of staff is receiving threatening or abusive phone calls or e-mails, it may be necessary for switchboard staff or the Information Security team to have access to personal data such as names or e-mails addresses in order to prevent further contact. They do

not need, however, to have full details of the record of previous abusive calls or messages.

12.3 Depending on the nature of an incident that give rise to the record, it may be necessary for OFMCO Departmental Security Unit and/or the police to have access to it. This would be the exception rather than the rule and the Team that produced the record should always query whether anyone outside the Team has a legitimate interest in accessing the information.

12.4 The registered file should be monitored every six months to remove records about individuals with whom no further contact is necessary or envisaged. The nature of the incident will dictate how long specific records are kept. The following retention periods will apply:

Nature of incident	**Retention Period**
Abusive	6 months
Sexual/malicious	12 months
Hoax	12 months
Bomb threats	12 months
Unacceptable internal calls	12 months

Annex A

RECORD OF AN UNACCEPTABLE TELEPHONE CALL

Name of person receiving call	
Branch	
Division	
Location	
Extension number	
Date of call	
Time of call	
Characteristics of call	
Background noise heard (e.g. outside/inside, office noise, TV/radio, conversation)	
Did the call sound like it was from a landline or a mobile?	
Vocal characteristics (e.g. type of accent, male/female voice)	
Did the caller use your name? If so, could they have obtained your name as part of your greeting or was it on a voicemail message?	
Did you recognise the voice?	
Was the phone ring external or internal? **NB** If the call was external contact the switchboard immediately to check if they can remember whether or not they had put a call through to your extension and if a name or number was quoted	

Please now forward this record to your line manager and to the HR Business Partner, and inform the WG Security Adviser if considered appropriate.

Signed:

Date: