EMPLOYMENT SCREENING GUIDANCE FOR THE WATER INDUSTRY

A report from the Water UK Personnel Security Working Group

Water UK

Version 1.0 2018

NOTE

This document is produced in response to the Defra document 'Security of Network and Information Systems' therefore covers English water companies. Water companies in Wales, Scotland and Northern Ireland may also find this guidance useful but consideration will need to be given to the specific legislation in these devolved administrations.

Version Control

Version 1.0: May 2018 – Initial distribution

Contents

Foreword

To provide the essential services of clean, safe drinking water and the removal and treating of wastewater requires water companies to take a holistic view to security. This includes the physical protection of sites, technical safeguards against the threats emerging from the cyber world through to the management of risk associated with staff that have access to such sites and systems.

This guidance document provides advice and support to companies to ensure that the staff they employ are properly screened and vetted to continue this holistic ethos into the realm of people.

Produced by people whose job it is to deliver this protection on a day to day basis, this document provides a valuable resource to practitioners across the industry.

J Marshall

Dr. Jim Marshall
Senior Policy Adviser
Water UK

Executive Summary

This document aims to provide guidance to the Water industry on employment screening and the standards that should be applied. Good employment screening is one aspect of Personnel Security which supports the holistic approach to managing overall security risk.

This paper looks at employment screening with specific reference to the new Security of Network and Information Systems legislation only. It is not designed to be prescriptive but offer enough information and advice to enable effective employment screening to be rolled out consistently across the sector.

This paper covers 4 main areas; background to Personnel Security, types of employment screening, risk assessment and considerations for implementation.

1: Introduction

The 'Security of Network and Information Systems' became UK legislation on the 10 May 18. This legislation applied to the Water sector and it covered the protection and integrity of a water company's Information Technology (IT) and Operational Technology (OT).

The penalties for failing to comply with the legislation could attract fines of a maximum of £17 million.

Traditionally, physical security has been the primary defence against threats to the sector. However, due to an evolving and improving understanding of protective security a holistic approach to security is needed to protect from the wide range of risks facing the water sector.

Personnel security and Information security are just as important as their respective physical controls and yet they are the two most immature areas and are in need of significant focus and investment.

Recognising the sector's need for further guidance and support in Personnel security, Water UK recently formed the Personnel Security Working Group. The aims of this group are to provide direction on Personnel security, advice on policy and help direct the strategic improvements required for the benefit of the whole of the UK Water sector.

This paper was created in order to provide guidance on implementing employment screening that is needed to help manage the Personnel security risks associated with a company's information and network systems only. This guidance provided should be applied to 3rd party suppliers, contractors and temporary staff as well as permanent colleagues. Whilst this guidance is aimed at a specific legislation, for true holistic security, an organisation's screening policy should cover *all* its high-risk posts.

1.1 Background

The Water Sector is part of the critical national infrastructure and, as such, its personnel (whether permanent, temporary, seconded, contractors or service partners) have access to a range of sensitive resources (people, information and physical assets). Organisations are therefore vulnerable to insider risk.

The insider is defined as 'a person who exploits, or has the intention to exploit, their legitimate access to an organisation's resources for unauthorised purposes'.

At worst insider acts may be related to terrorism, espionage, sabotage or serious organised crime, but vulnerabilities are also exploited by disaffected insiders. As organisations implement increasingly sophisticated physical and information security measures to protect their resources from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

Personnel security is an integral part of the holistic approach to security and it is a system of policies and procedures which seeks to:

- reduce the risk of recruiting staff who are likely to present a security concern;

- minimise the likelihood of existing employees becoming a security concern;
- reduce the risk of insider activity, protect the organisation's resources and, where necessary, carry out investigations to resolve suspicions or provide evidence for disciplinary procedures;
- Implement security measures in a way that is proportionate to the risk.

The purpose of Personnel security controls (such as recruitment checks or national security vetting) is to minimise the insider risk by confirming the identity of individuals (employees and contractors) and providing a level of assurance as to their trustworthiness, integrity and reliability.

The reasons why staff can become a threat to an organisation are varied but the Centre for the Protection of National Infrastructure (CPNI's) *Insider Data Collection Study* shows that insider behaviour is shaped by a complex mix of factors including life history and the work environment. Certain factors may increase an organisation's vulnerability to insider activity, including:

- inadequate personnel security measures during pre-employment screening;
- inadequate ongoing personnel security measures, limiting the organisation's ability to identify or prevent insider activity among its employees;
- poor management practices, which may reduce employee loyalty and commitment;
- ineffective grievance processes for employees to voice discontent before it escalates into disaffection;
- lack of a strong security culture, resulting in employees not taking individual responsibility for security and reduced compliance with security procedures.

Effective Personnel security measures can help organisations to assess the suitability of personnel to access sensitive assets and resources. A suitable person demonstrates integrity and reliability and is not vulnerable to improper influence.

To provide effective Personnel security requires focus to 3 main components:

1. Pre-employment screening
    a. Employment checks - Identity proofing; Eligibility; Qualification checks; Previous employment checks/ references; Specific checks e.g. credit checks, drug screening etc.
    b. Initial security clearances
2. Managing on-going suitability
    a. Education & Awareness - Countering manipulation; Security culture
    b. Monitoring & Evaluation - Access controls; Protective monitoring; Investigations; Ongoing employment suitability checks; Security clearance maintenance
    c. Access Control – based on roles not people. Starters, movers, leavers
3. Severance activities
    a. On-going obligations briefing - Exit interview; Leavers letter
    b. Withdrawal of access and retrieval of assets
    c. Security clearance actions i.e. notification to relevant authorities

This paper specifically focuses on the pre-employment screening aspects of Personnel security.

1.2 Reporting

In order that the sector can learn, develop and adapt to the evolving risks associated with security breaches committed by personnel, it is vital that consistent reporting routes exist for all breaches of security (of any kind) whereby information can be shared with a range of stakeholders. Water companies are working with Defra and its advisors to clarify reporting lines for incidents that escalate above 'routine' operations with the aim of establishing a single, consistent approach.

2: About this document

This document is the result of the Water UK Personnel Security Working Group's efforts, and it provides the collective view on what good practice should look like for employment screening in managing the risks to the water sector's critical services. This document has been written for human resources (HR), security personnel and those with line management responsibilities, all of whom have a role in creating and maintaining a culture of effective ongoing Personnel security.

2.1 Scope and purpose

The scope of this paper includes roles of a higher risk that could directly affect a water company's critical services relating to the NIS. All roles specific to each company should be identified through an assessment of insider risks. The information in this paper is not intended to be a fully comprehensive and complete instruction to follow but provides guidance on what good looks like and the approach to take. This guidance does not look at all of the other roles and insider risks that a company may have. The employment screening guidance in this document should be viewed as one segment in the whole holistic security model.

2.2 Use of document

This document is meant as a practical reference guide to best practice. It is not exhaustive but sets out the recommended standards to use.

3: Types of Employment Screening

Conducting pre-employment checks on job applicants is an integral part of the recruitment process. Careless approaches to vetting and screening risk employing the wrong people. However, a balance must be struck, and the laws on discrimination and data protection must be considered at its core.

In conducting employment checks, employers should aim to:

- Protect the organisation
- Protect staff
- Protect customers
- Be fair to all candidates
- Ensure non-discrimination and compliance with data protection law
- Rely on fact, not opinion
- Validate information to be relied upon
- Ensure relevance to the post to be filled
- Be transparent and open to candidates about the checking process

When implementing employment checks, it is recommended that legal advice is sought in order to ensure that employment checks are done in a legal and ethical manner that complies with the law. There are limits on an employer's ability to lawfully obtain and act upon personal information regarding an applicant's criminal or medical history. Typically, checks should be made only once a successful applicant has been chosen, as a condition of an offer of employment. Employers should also take care only to request information from an applicant that is relevant to his application, and should make it clear to applicants how and when such information will be processed and verified.

There are a variety of employment checks available to employers. These checks should be relevant and proportionate to the role being recruited. A minimum standard of pre-employment checks should be completed for all roles and a risk assessment undertaken to determine what roles require further checks.

There are some minimum pre-employment checks required by law and some basic good practice checks. The aim being to confirm that the person is who they claim to be. These include:

- Identity check
- Right to work in the UK
- Criminal records self-declaration
- Proof of address history
- Reference checks– covering the last three years of employment. Where there are gaps in a candidates employment history these should be explored and verified where possible.

As these checks should be undertaken as routine business, they will not be addressed further in this paper. Furthermore, there are other employment checks available which will help mitigate against business risks, these include:

- Professional Qualifications
- Directors Check
- Media Check
- Credit Check

The benefits and justification of using these checks will be determined after undertaking a role risk assessment. For the purpose of this document, they will not be addressed further in this paper.

The following checks are specifically referenced as a means to manage higher risk roles around network and information systems.

Type of Check	Comments
Basic Disclosure	The Disclosure and Barring Service (DBS) as of the 1 Sep 2017 now undertakes basic criminal record checks for people in England & Wales. This replaces the service previously provided by Disclosure Scotland. An online process for individuals is expected to be in place from 1 Jan 2018. A basic disclosure shows any 'unspent' criminal convictions in the UK. Under the Rehabilitation of Offenders Act 1974, some convictions can be treated as 'spent' meaning they are not relevant to basic disclosure after a certain length of time. If a conviction has become spent then the employer must treat the applicant as if the conviction has not happened. This check does not access criminal records held overseas. There will be two ways of getting a basic check from the DBS: Option 1 – The applicant applies directly to the DBS – This is via an online self-service channel run

	by the DBS. Option 2 – The applicant applies via their employer or other registered organisation – This is where the applicant applies via an organisation registered with the DBS (referred to by the DBS as a "responsible organisation") who are allowed to submit applications for basic checks via a DBS web service. Cost of a Basic Disclosure is £25, however a 3rd party providing this service may charge more.
Standard Disclosure	A standard disclosure shows any 'unspent and spent' criminal convictions, cautions, reprimands and final warnings in the UK. Access to this service is only for employers who are entitled by law to ask an individual to reveal their full criminal history. This is known as asking 'an exempted question'. An exempted question applies when the individual will be working in specific occupations. These are covered by the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. The Exceptions Order identifies the exceptions, which fall into five broad groups: • Professions • Those employed to uphold the law • Certain regulated occupations • Those who work with children, provide care services to vulnerable adults or who provide health services • Those whose work means they could pose a risk to national security Applicants who fall within the scope of the Exceptions Order qualify for checking through the Disclosure and Barring Service (DBS). Organisations receiving standard or enhanced disclosure information must abide by DBS code of practice for registered persons and other recipients of disclosure information. Information revealed should only be considered for the purpose for which it was obtained and it should be destroyed after a suitable period has passed, usually no more than 6 months. Cost of a Standard disclosure is £26, however a 3rd party providing this service may charge more.
Enhanced Disclosure	An Enhanced Disclosure can only be undertaken for specific roles, such as those working with direct unaccompanied access to children or vulnerable adults. It shows the same information as a standard a check plus any information held by the Police that's considered relevant to the role. The same rules that apply to a Standard Disclosure, also apply to an Enhanced Disclosure. Cost of an Enhanced disclosure is £44, however a 3rd party providing this service may charge more.
Overseas criminal record checks	Full guidance on how to obtain criminal records disclosure on individuals in 63 countries can be found in the CPNI guidance 'How to obtain an Overseas Criminal Record Check' here. The application process for obtaining criminal record checks varies significantly between countries.
BS7858	The BS7858:2012 is a Security screening for individuals employed in a security environment. This British Standard gives recommendations for the security screening of individuals to be employed in an environment where the security and/or safety of people, goods and services, personal data or property is a requirement of the employing organization's operations and/or where such security screening is in the public and/or corporate interest. This check comprises the following: • Identity checks • Financial checks • Employment checks and details of education • Criminal records (basic disclosure) • Checking of a character reference As this standard is made up of a number of checks, prices will vary depending on who conducts them.
Baseline Personnel Security Standard	The BPSS is not a security clearance but the minimum background screening check set out by the government, used for positions that would be working within or on behalf of a government department and is a basic entry-level standard that organisations in several sectors are expected

(BPSS)	to meet. The BPSS was created to help mitigate the risk of identity fraud, reduce the number of illegal workers, and to protect national security. The BPSS outlines the pre-employment background checks that all civil servants, members of the armed forces, temporary staff and government contractors must undergo before they are granted access to government assets. The BPSS comprises the following checks: • Identity checks (& ID conformation) • Nationality and immigration status / right to work • 3 years employment checks / references • Criminal record checks (basic disclosure) As this standard is made up of a number of checks, prices will vary depending on who conducts them. For higher risk roles it is recommended that a BPSS + (Enhanced) is considered. This could include the following checks: • *Identity checks (& ID conformation)* • *Right to work* • *3 years employment checks / references* • *Criminal record checks (basic disclosure)* • Current address check • 5 year address history • Employment gap analysis • Personal credit history • Internet mining search • Sanctions search
Counter Terrorism Check (CTC)	A Counter Terrorist Check (CTC) is required to reduce the risk of anyone with known terrorist activity having access to sensitive information or valuable assets. A CTC is carried out if an individual is working in proximity to public figures, or requires unescorted access to certain military, civil, industrial or commercial establishments assessed to be at particular risk from terrorist attack. A CTC Clearance level does not allow access to, or knowledge or custody of, protectively marked assets, but the Baseline Personnel Security Standard allows a degree of access. The CTC Clearance process involves the following mandatory stages: • BPSS, which is normally undertaken as part of the recruiting process • Departmental / Company Records Check • Security Questionnaire • Criminal Record Check • Security Service Check To gain CTC clearance, applicants will usually need to have been a UK resident for a minimum of 3 years. A CTC is usually valid for 3 years.
Security Clearance (SC)	The United Kingdom Security Vetting (UKSV) launched on 1 Jan 2017 to establish a single provider of government National Security Vetting Services. A SC determines that a person's character and personal circumstances are such that they can be trusted to work in a position which involves long-term, frequent and uncontrolled access to SECRET assets. To get a SC, individuals must be sponsored to apply for a Security Clearance. Your sponsor is someone who is required to verify that the BPSS was done prior to your employment and can also verify that your role requires you to have the identified level of clearance. A full Security Check clearance process comprises: • BPSS, which is normally undertaken as part of the recruiting process • Departmental / Company Records Check

	• Security Questionnaire • Criminal Record Check • Credit Reference Check • Security Service Check On completion of the process, the information collected is assessed and a decision made to refuse or approve an SC. The clearance process can take between 1-3 months to complete prior to the candidate starting work. Gaining Security Clearance will normally require you to have been a resident in the UK for a minimum of 5 years. A SC is typically valid between 5-10 years. Aftercare is the term used for the maintenance of effective personnel security. Its purpose is to investigate and monitor anything of continuing security concern, between periods of normal review, which could affect an individual holding a NSV clearance.

4: Risk Assessments

The most important stage of understanding what employment screening checks are needed will come from undertaking a risk assessment. This should be a two stage process. It should start with the identification of the organisational assets that need to be protected and an assessment of the risks to those assets from (any) potential insider. The identification of high-risk roles should then flow from that. The risks of each role should be evaluated based on the access and therefore the opportunity afforded by the role; on whether the post-holder would have the necessary capability to exploit their access; and on the effect on the business if this position were to be exploited.

The scale of this inherent risk will help determine what employment checks are needed in order to help ensure that only the right, trustworthy people are given the appropriate privileges. Further risk mitigation is achieved by following the other Personnel security principals such as access control etc.

Whilst not intended to cover every role within the water sector, the following table gives an illustrative model on what higher risk roles could be considered in order to protect a company's information and network systems and their associated employment checks. This guide is intended to show what is considered to be good practice in terms of the standards of associated employment checks to be used.

		Risk Assessment									
Role	Risk (Vulnerability) Discription	Probability of Occurrence (likelihood)	Impact (consequence)	Risk score & RAG Status	Basic Disclosure	Standard Disclosure	Enhanced Disclosure	BS7858 checks	Baseline Personnel Security Standard	CTC	Security Check
Privileged Security staff	Key security staff are given a large amount of access, are privy to very sensitive company information, are intimately aware of key vulnerabilities and have the opportunities to exploit these weaknesses If this information were to be exploited then significant. harm could occur to the business. Statistically, security staff are among the 3 highest areas of risk for reported insider activity. As security staff will likely have knowledge of the CNI sites and other sensitive information within the business then it is suggested that they have a Security Clearance.	Low	Very high		x (inculded as part of the BPSS)				X+		X
Privileged SCADA , network & telemetry staff	SCADA systems control the water process and water network. Malicious use of this system could result in a major pollution event, danger to public health, significant reputational damage and fines to the company.	Low	Very high		x (inculded as part of the BPSS)				X+	X	
Privileged Data Centre & IT staff	Key IT and data centre staff are privileged with significant access and control over a company's sensitive information and IT network. Malicious use of this system could result in significant disruption to a business, reputational damage and fines to the company.	Low	Very high		x (inculded as part of the BPSS)				X+	X	
Guards	Security staff are often given unsupervised access, are privy to sensitive company information, are aware of some key vulnerabilities and have the opportunities to exploit these weaknesses If this information were to be exploited then significant. harm could occur to the business. Statistically, security staff are among the 3 highest areas of risk for reported insider activity.	Low	High		x (inculded as part of the BPSS)			X		X (AMC staff)	
Staff responsible for multiple CNI sites	Staff responsible for multiple CNI sites can gain the knowledge and access to exploit these critical sites. With malicious intent this could led to significant disruption to a business, harm to the public, reputational damage and fines to the company. It is a Defra requirement that anyone who has knowledge of 2 or more CNI sites should be CTC cleared.	Low	high		x (inculded as part of the BPSS)				X+	X	
Frontline SCADA , network & telemetry staff	SCADA systems control the water process and water network. Malicious use of this system could result in a major pollution event, danger to public health, significant reputational damage and fines to the company.	Low	Medium		x (inculded as part of the BPSS)				X		
Frontline IT staff	IT staff can be privileged with significant access and control over a company's sensitive information and IT network. Malicious use of this system could result in significant disruption to a business, reputational damage and fines to the company.	Low	Medium		x (inculded as part of the BPSS)				X		
Front line operational staff with access to key network systems	SCADA systems control the water process and water network. Malicious use of this system could result in a major pollution event, danger to public health, significant reputational damage and fines to the company.	Low	Medium		x (inculded as part of the BPSS)				X		

The BPSS should be considered as the minimum standard required. Higher risk roles annotated as 'X+' should be given BPSS Enhanced checks.

5: Considerations

In-house or outsourcing and Data Protection

The decision on whether to outsource employment checks or undertake them in-house will typically be based on time, resources and cost. However, consideration should also be taken to data protection and the control, storage and deletion of personal data and the legality issues associated with employment checks. Often the well-established and recommended professionals in the employment checks arena cover these two areas well, therefore reducing the burden on companies. Secure record keeping will be required so that the person, role they are in, type of vetting, date of vetting and its expiry, and outcome is recorded. The length these records are kept will be in accordance with General Data Protection Regulations (GDPR).

Stakeholders

HR, security, business owners and managers, and lawyers will all contribute to the screening process but it is advisable for one department to take the lead.

Gathering the Information

The use of a standardised application form will enable organisations to collect most, if not all, the information required from an applicant. Interviews also play an integral part in the pre-employment screening process: they encourage the applicant to be honest, allow the employer to fill in any gaps in the information provided/probe the responses, and provide a good opportunity to add to the overall assessment of the applicant's reliability and integrity.

Dealing with adverse outcomes from checks

Companies also need to consider how they will deal with any 'adverse' outcomes from checks and it may be useful to put some governance in place to guide decisions on what could be considered acceptable. The decision as to whether it is appropriate to employ a candidate in a particular role should be made following careful consideration of all the facts.

Issues with Vetting Potential and Existing Staff

There are a number of potential issues with rolling out a security vetting programme to potential employees; employees moving into a new role; and employees who are currently not vetted but are in roles that may be assessed to require enhanced vetting. This is not deemed to be an exhaustive list, but the below may serve to highlight and illustrate some of the potential issues and conflict points:

a. A believed infringement of human rights;
b. An individual's concern over a spent or unspent criminal record being discovered;
c. Personal information being misused or misappropriated;
d. Contravening a person's right of privacy; and
e. Breaking of contractual agreement

If an individual does not comply with an associated employment check, then it may require a risk assessment of an individual to determine whether this person is allowed to access sensitive information and assets.

If an organisation fully aligns itself to these checks, and there is a refusal to either participate, or a non-compliance from either a future employee or an existing member of staff, this may lead a company to refuse the application; or prevent the existing employee from either remaining in a role, or moving to a new role. In a worst case scenario, it may require the termination of employment for that individual.

With the above points in mind, there is a possibility that individuals may become hostile to vetting, leading to possible grievances and Trade Unions involvement.

Consideration should be given to the risks involved in vetting staff already in role and the risks to the business if only new starters and new movers were considered for employment checks.

A number of these risks can be mitigated by having clear rationale for any vetting to be undertaken and clear outcomes, including:

- A vetting policy and procedure;
- Involvement of Trade Unions;
- Clear decision making.

It must be clearly articulated who would have knowledge of any adverse findings. Traditionally, HR would decide and confirm clearance where the issue is deemed not relevant to the role or the risk is minimal (based on nature of conviction, penalty, how long ago it was) OR make a recommendation that the employee is redeployed or has restrictions within the role applied.

A manager typically would not be told of the nature of the conviction. Prior to vetting being implemented, suitable roles for potential redeployment should be considered in the event of adverse findings.

Appeals

Existing employees have a right of appeal against a decision to refuse or withdraw a National Security Vetting (NSV) clearance. Internal appeals processes should include an ultimate right of appeal to the Head of Department (or equivalent). If the decision is upheld there is a further avenue of appeal to the independent Security Vetting Appeals Panel (SVAP)1. The panel is available to all those (other than external applicants for employment) in the public and private sectors subject to NSV.

Managing the risk

Identifying risks that comes out from an employment check should not automatically mean that an individual is unsuitable for a role. A risk assessment should be made of the findings and an assessment made to see if the risks can be managed. It may also mean that one role is unsuitable but another is suitable. Consideration should be made to how the ongoing risk management of

[1] SVAP is currently located at:
http://webarchive.nationalarchives.gov.uk/+/www.direct.gov.uk/en/DI1/Directories/DG_065029

individuals throughout their time in a company would be managed when higher risk individuals are identified.

Managing Security Clearances

There are specific requirements needed in order to manage security clearances such as an annual review of people's circumstances and a debrief of individuals when they leave the business. Security clearance holders should report all changes in circumstances and any suspicious, ongoing, unusual or persistent contacts. Managers responsible for such personnel should report any concerns about the clearance holder. The person administrating the security clearances must also hold a security clearance themselves.

Through Life vetting

Pre-employment checks help reduce the risk of getting inappropriate individuals into a new role. However, employment checks only give an indication of someone's suitability at the time of the check. Many insider acts are carried out by individuals who have been in a company for many years. Circumstances change and external influences over time can lead individuals to exploit their position at work. Because of this, consideration should be made to ongoing employment checks for individuals who stay in role over a long time.

Service Partners / Third Party Contractors

The principles of employment screening should equally apply to contractors, service partners and 3rd parties that have the same access to sensitive assets and information as permanent company staff. This in itself presents further contractual considerations in how it would be implemented to current and future contracts. This will be considered in another paper.

Links and resources

Personnel Security Advice

http://www.cpni.gov.uk/advice/Personnel-security1/Screening/

http://www.cpni.gov.uk/advice/Personnel-security1/Disclosure-employee-related-info/

http://webarchive.nationalarchives.gov.uk/+/www.direct.gov.uk/en/Dl1/Directories/DG_065029

Pre-employment Checks

Disclosure and Barring Service (DBS)

https://www.gov.uk/government/organisations/disclosure-and-barring-service

Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975

https://www.legislation.gov.uk/uksi/1975/1023/contents/made

Disclosure Scotland

http://www.disclosurescotland.co.uk/

CPNI guidance 'How to obtain an Overseas Criminal Record Check'

https://www.cpni.gov.uk/system/files/documents/42/ca/how-to-obtain-an-overseas-criminal-records-check.pdf

UK Security Vetting

https://www.gov.uk/security-vetting-and-clearance

Completing your SC / CTC application

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/437985/20150623-NSV_Subject_Guide_CTC-SC.pdf

https://www.gov.uk/government/publications/security-policy-framework

Other

European legislation The Directive on security of network and information systems (NIS Directive) - https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive

For Water Companies

Affinity Water
Bournemouth Water
Bristol Water
Cambridge Water (South Staffs)
Cholderton and District Water
Dee Valley Water
Essex & Suffolk Water (Northumbrian)
Hartlepool Water (Anglian)
Portsmouth Water
South East Water
South Staffs Water
SES Water

Anglian Water (Hartlepool Water)
Dŵr Cymru - Welsh Water
Northern Ireland Water

Northumbrian Water
Scottish Water
Severn Trent Water
South West Water
Southern Water
Thames Water
United Utilities
Wessex Water
Yorkshire Water

Albion Water
Independent Water Networks
Peel Water Networks
SSE Water
Thames Water Commercial Services
Veolia Water Projects

For Defra

Jessica.Curzon@defra.gsi.gov.uk

For CPNI

ChrisJ@cpni.gsi.gov.uk