Communication Routes

Dealing with sensitive and private information means that services must take their responsibilities seriously in meeting the requirements of the Data Protection Act. Information handled within Human Resources (HR) is generally of a sensitive nature, for example; the outcome of grievances, an individual's bank account details or their ID evidence. Therefore, data security and protection along with confidentiality is a significant element of the work undertaken within HR. When dealing with communications into or out of a service, it is important to consider the level of protection required to ensure the information is sent or received successfully.

Sensitive Information

Sensitive information is any information that is seen as personal to an individual or group of individuals. This information may be personal or contractual details, or information relating to services that the individual may not wish to have released. Further details on this can be found on the Information Security section of the intranet.

Employee personal data is regarded as sensitive and should only be provided to those who are authorised. Managers and the employee can have access to all information held on their file unless it is classified as confidential (and states such), for example; references will not be released to an employee where they are marked as confidential. Any other employees, friends or managers not in the line management structure of that employee should not be given such access unless this has been agreed with your manager or an appropriate member of HR. This information includes; employee contact address, telephone numbers and email.

Protective Markings

Protective marking of documents is used to identify where sensitive or personal information is contained, and this is normally denoted by the terms 'protect' where information relates to an individual or 'restricted' where it relates to more than one individual. All HR documents are protectively marked as appropriate. Further details on this can be found on the Information Security section of the intranet.

Third Parties

Protective marking of documents is used to identify where sensitive or personal information is contained, and this is normally denoted by the terms 'protect' where information relates to an individual or 'restricted' where it relates to more than one individual. All HR documents are protectively marked as appropriate. Further details

on this can be found on the Information Security section of the intranet.

Postal Mail

Mail continues to be a well-used form of communication, particularly where documents are required with a signature or where an individual does not have access to electronic communication. When using mail as a communication route, it is appropriate to use the most cost-effective method in order to reduce costs whilst retaining data security.

Where information is being sent out of a service, or is being sent to that service, the same requirements apply and the service must ensure that customers are aware of this. For example; all information should be sent by standard mail (normally second class) unless it contains sensitive information, at which point the information should be sent by recorded delivery. If the contents are valuable e.g. identification documents such as a passport, then other methods of communication should be considered (in person) or the use of special delivery or couriers may be preferable. Remember: sensitive information is not all personal information and so Contracts of Employment may still be sent through normal mail, but not where it includes other sensitive information such as date of birth, national insurance details etc.

At the HR Service Centre (Barrack Street) incoming mail will always be opened and date stamped, without exception. At other sites, this may be different. All mail being hand delivered should also be date stamped by the team concerned or placed in the post tray for processing and date stamping. Any mail marked as ‘private’ or ‘strictly private and confidential’ will not be opened but instead will be passed to the team, or individual whom it is addressed to. This mechanism should only be used for those documents that really are private or personal and anyone using this route for general documentation or information will be challenged.

Telephone

Telephone communication is not automatically secure and so if you wish to exchange sensitive information with someone over the telephone then it is essential that the individual on the other end of the line is able to confirm personal details in order to validate their identity. Ideally three unique pieces of personal information should be provided to confirm an identity e.g. date of birth, assignment number, national insurance number, full postal address etc. If this is not possible, then telephone communications relating to sensitive information should not be used.

Email

Warwickshire County Council operates a fully secure email system which means that any emails to and from a warwickshire.gov.uk email address to another warwickshire.gov.uk email address will be secure. However, this is not necessarily

the same for emails sent from a warwickshire.gov.uk email address to any other email address (and vice versa).

Email addresses which can be used to securely email, or be securely emailed to, are;

@we-learn.com
@welearn365.com
@avonvalleyschool.org
@cawston.warwickshire.sch.uk
@etone.org.uk
@george-eliot.org.uk
@harris-school.co.uk
@hartshill.warwickshire.sch.uk
@haselor.warwickshire.sch.uk
@ilmington.warwickshire.sch.uk
@kingedwardvi.warwickshire.sch.uk
@kingsbury1stplaygroup.org.uk
@northleamington.co.uk
@ourladysrc.warwickshire.sch.uk
@queenelizabeth.warwickshire.sch.uk
@raceleys-jun.warwickshire.sch.uk
@shipston.warwickshire.sch.uk
@st-benedicts.org
@st-nicolas.warwickshire.sch.uk

Any **other email addresses are not secure**, including popular email addresses such as;

@hotmail.co.uk
@btinternet.com
@google.co.uk

For Central Government, or other Government organisations, then any email address where the letters 'gcsx' appears in the email address is secure, for example; @government.gcsx.gov.uk. Any other email addresses e.g. @government.gov.uk is not secure and so should not be used for confidential information. Where Government, or other Government organisations, wish to send information to Warwickshire County Council then they will need to send the email to emailaddress@warwickshire.gcsx.gov.uk in order to ensure it is secure. Sending emails from a 'gcsx' to a normal @warwickshire.gov.uk email address is not secure. The receipt and sending of 'gcsx' secure emails must be done through Lotus Notes and cannot be done through Google mail.

For NHS organisations, the email addresses using the domain @location.nhs.net are secure to warwickshire.gcsx.gov.uk as with Central Government above, however other nhs email domains, including @location.nhs.uk are not yet secure and so cannot be used to send or received sensitive information.

HR and Payroll direct and Forms direct

HR and Payroll have rolled out electronic forms for the submission of payroll and HR transactions; these requests contain sensitive information and as such are transmitted via a secure link (API) to our workload management system. Emails from this system will not contain sensitive information as these emails are outside of the warwickshire.gov.uk email network therefore are not within the secured network.

Any secure information submitted to the HR and Payroll service must be sent via a relevant e-Form or sent to a warwickshire.gov.uk address, sensitive information sent from HR and Payroll will be via a secure email address or encrypted using 256bit encryption.

We are here to help

For assistance please contact the HR and Payroll direct;
Email: hrandpayrolldirect@warwickshire.gov.uk
or
Tel.: 01926 738444