Data Protection Policy

Contents

Introduction

This policy sets out how Cross Connecting directors, staff, consultants, contractors, and volunteers use and protect the personal information that is provided to us.

Cross Connecting is committed to protecting all information entrusted to us and complies with all data protection and privacy legislation or regulations including Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR") and the Data Protection Act 2018.

Cross Connecting is a data controller. This policy covers the capture, storage, processing, management, distribution and secure destruction of personal data for people connected with, taking part, or otherwise supporting Cross Connecting. It is ordered so that the earlier sections are relevant to the most people.

Purpose

The purpose of this policy is to ensure that Cross Connecting, its staff, directors, and volunteers understand their obligations and rights in regard to:

- complying with legislation, regulations and good practice
- protecting those who attend our events or are connected to the organisation in some way that require the disclosure of personal data
- respecting the rights of individuals and being open and honest with them.

Importance

Our personal information and data is important to us all. Cross Connecting care deeply about people's wellbeing and how we protect personal data. It is fundamental to our integrity and the public's confidence in us as an organisation.

Failure to comply with this policy will increase the risk to children, parents, supporters, volunteers, and staff. Failure to comply could also lead to fines. Cross Connecting may also be asked to pay damages to people impacted by any breach of this policy. The importance of complying with this policy should not be under-estimated.

As a result, team members who do not comply with this policy may be subject to disciplinary action and volunteers who do not comply may be asked to leave their role.

Breaches of Data Protection

Personal data breaches can include:

- access by an unauthorised third party,
- deliberate or accidental action (or inaction) by Cross Connecting staff or volunteers or an external data processor,
- sending personal data to an incorrect recipient,
- computing devices containing personal data being lost or stolen,
- alteration of personal data without permission, or
- loss of availability of personal data.

If a breach occurs whether by accident or otherwise, whether by yourself or others, you must inform the Cross Connecting directors immediately. They will investigate the nature of the breach and document the number of people impacted, the categories of personal data affected, the proposed mitigation, the possible consequences, and organise any steps to prevent further breaches.

They will establish the likelihood and severity of the risk to people's rights and freedoms – physical, material or non-material damage, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage.

If it is likely that there will be adverse consequences to people, Cross Connecting will notify the affected individuals without undue delay, provide advice to help protect from the effect of the breach, and will inform the Information Commissioner's Office within 72 hours.

Data Processing

Definition

Personal data is any data that can partially, indirectly or directly help identify a person, whether an adult or a child. Photographs, addresses, religious affiliation, twitter address, IP addresses, videos, recordings, medical details are all examples of personal data that is covered by the Law, whether named or not. The data can be on paper or held electronically.

Data Processes

Cross Connecting process and hold personal data provided by people for:

a) using the Cross Connecting digital platform
b) volunteering with Cross Connecting, including receiving prayer news
c) donating to Cross Connecting
d) booking onto our events

e) making an online order
f) staying in touch and maintaining relationships
g) paying staff, suppliers and expenses

Deceased Individuals

Although the GDPR legislation does not cover deceased individuals, we apply the same policies and procedures as for living individuals.

Special data categories and protections

In law there are special categories of data with special protections. These categories are race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation. Cross Connecting will not capture, process or hold such data without documenting in advance the lawful basis for processing the data (as with all personal data), but also documenting a separate, valid condition in law for processing that special category data. These special category data conditions are:

a) explicit consent from the person;

b) for employment, social security or social protection as authorised in law;

c) to protect the vital interests of the person where they are physically or legally incapable of giving consent;

d) processing that relates solely to our members or former members, or to people who have regular contact with us, in connection with our purposes and that the personal data is not disclosed externally without the consent of the people;

e) the data is already manifestly made public by the person;

f) the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g) in the substantial public interest;

h) for preventive or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, health, social care, treatment or the management of health or social care systems and services, or a contract with a health professional - all as authorised in law;

i) for the public interest in public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices – as authorised in law; and

j) necessary for archiving in the public interest, scientific or historical research purposes, or statistical purposes, as authorised in law.

We process and hold some of these special categories of data:

(i) If an individual's personal data with Cross Connecting was to be accessed without authorisation, that person's religious belief could be inferred - a special category of data in law. So Cross Connecting has a legal duty to provide special protection for all of the personal data held by us.

(ii) We could also process job and volunteer application forms where we request information on criminal offences, again with the applicant's explicit consent.

Our Responsibilities

Cross Connecting is responsible for complying, and demonstrating its compliance, with the six principles outlined in the GDPR.

Processing personal information lawfully, fairly, accurately and transparently

- We will be honest and open about why information is provided or requested, what we will use it for, including the third parties who will have access to the data.
- We are committed to data privacy: if personal information is provided or requested by data subjects, people can be made aware of their rights to access, correct, transfer, delete (the right to be forgotten) or change the way we process their data.
- For children under the age of 18, we will seek and record the consent of their parent, legal guardian, or loco parentis when first granted permission by the parent or legal guardian.
- We separate out multiple purposes for data processing and allowing separate consent for each, including future contact.
- We disclose personal data to authorised government authorities when we are required to do so because of an applicable law, court order or governmental regulation, or if such disclosure is otherwise necessary in support of any criminal or other legal investigation or proceeding, here or abroad.
- To respect the privacy of our supporters and the integrity of the information trusted to us, we do not append externally-sourced data to people's

information, and we do not use artificial intelligence to make automated decisions about the services and costs that offered to people.

Collecting and processing *only* the personal information that is needed to carry out our work or comply with legal requirements

- Personal data cannot be collected for one purpose and then used for another. If we need to change the purpose, we should secure consent from the individual in advance.
- We respect the privacy of our friends and supporters and do not append externally-sourced data to individual's information, and we do not use artificial intelligence to make automated decisions about the services and costs that we offer to people.

Processing personal information adequately, relevantly and limited to what is necessary for the documented purposes

- We take particular care in processing and storing high risk data such as payment information, sensitive or special category data, details of criminal offences and information relating to children.
- All information will be factual and evidenced to avoid the risk of any legal action because of expressions of opinion or unsubstantiated comments.

Keeping information up-to-date

Where data is known to be inaccurate, we take reasonable steps to rectify the inaccuracy or delete the data concerned.

Holding personal information for *only* as long as is necessary

See *Error! Reference source not found.*.

Taking data security very seriously

The following principles apply with respect to data security:

- Confidentiality - protecting against unauthorised or unlawful processing.
- Integrity - protecting against accidental loss, destruction or damage to data:
    i) by keeping personal data accurate, complete and suitable for the purpose for which it is to be processed; and
    ii) by carrying out data protection impact assessments during the planning of any significant changes to our work, systems,

resources, locations or processes, taking a “data protection by design” approach.

- Availability - authorised users should be able to access the data they need for authorised purposes.

Responsibilities by role

The Directors and Data Protection Officer (DPO)

The Directors are accountable for data protection and delegate day-to-day responsibility to the Data Protection Officer (who could also be a director).

Cross Connecting provide adequate resources for the DPO to meet the responsibilities below and they cannot be dismissed or penalised for performing their duties.

These responsibilities include:

a) briefing the Directors on Data Protection responsibilities and compliance
b) reviewing the Data Protection Policy
c) informing and advising staff and volunteers about their obligations
d) monitoring data protection induction, training and compliance, including internal data protection activities
e) advising on data protection impact assessments
f) training staff and volunteers
g) conducting internal audits
h) completing periodic reviews, reviewing compliance returns, updating the Risk Register and writing reports for the directors as needed
i) being the first point of contact for supervisory authorities, recording breaches and reporting as required to the Information Commissioner’s Office
j) managing requests from contacts, staff and volunteers for data access, rectification, transfer and deletion, as well as requests to stop or amend data processing
k) approving unusual or potentially controversial disclosures of personal data
l) approving contracts with external data processors

Leaders and managers

The DPO delegates responsibilities for Data Protection compliance and demonstrating compliance as needed. This refers to situations where our direct contracted partners in the delivery of our services requires access to personal data (such as leading youth groups and requiring access to personal data). The delegated responsibilities are:

a) maintaining up-to-date and fit-for-purpose operational procedures for all activities

b) training volunteers before they capture, process, amend or otherwise access any personal data so that they can work confidently, accurately, securely and consistently

c) supervising teams, assessing the performance of each team member through regular observation and checks

d) managing the personal data that is in the care of the team, complying with this policy at all times

e) completing compliance returns when appointed and thereafter, on time and in full, to the DPO

All staff and volunteers

Team members, whether staff and volunteers, have the following responsibilities:

a) reading, understanding and agreeing to follow this policy and procedures

b) if uncertain or unclear about what to do, seeking help from their manager/leader *before* responding to a query or processing data

c) the operational security of all systems and apps that are used

d) obtaining and recording the consent of parents or legal guardians of children aged under 18 to process their data, including photos and videos, on application forms and other permission forms

e) immediately reporting all breaches of this policy or procedures to the Data Protection Officer, whether accidental or otherwise, by themselves or others.

Data Security

This section sets out how Cross Connecting preserves the confidentiality, integrity and availability of personal information.

Passwords

Passwords are critical for securing personal data. All directors, staff, contractors, and volunteers have a responsibility to choose strong passwords, to keep them secure and to never share them with anyone.

a) All users will have uniquely named user accounts. Generic accounts will not be used.

b) Passwords must be different for each email account.

c) Strong passwords have 10 characters or more, include random words, lower case letters, upper case letters, numbers, and spaces and/or symbols if allowed - but they do not replace letters with them.

d) Two-factor authentication must be used wherever it is available – an account becomes accessible only on registered devices. When someone logs in using a new device, you are asked to verify who they are, by for example entering a unique code which is sent to your mobile phone. If the person isn't you, they won't be given access because they shouldn't have your mobile phone with the unique code.

e) Do not include names in passwords that can be traced easily, such as your town, street, pet, birthplace, holiday place, nickname, name of someone related to you, someone or something related to your favourite sports team, or similar.

f) Do not leave notes or papers with passwords on your computer, desk, in work pads, phones or files. If you record your passwords in a secret place, there should be no reference to Cross Connecting or similar, no reference to them being passwords, and no mention of the systems or websites that the passwords relate to. They should be encrypted.

Preventing dangerous unauthorised release of personal data

a) The identity of any person or caller must be verified before any personal information is disclosed. All staff and volunteers **must** complete our data protection checks on everyone ***before*** providing or updating any information that we hold about them.

b) Do not allow yourself to be bullied into providing information. Let the person know that you will check with your manager/leader.

c) We must not give any individual's personal data to others - even contact information. Instead we should offer to contact the person requested and give them the name and contact details of the enquirer. If the enquirer will not agree, then no further assistance should be given.

d) **Only** employees, authorised contractors & volunteers, and authorised third-party data processors can be given any access to any personal data. If in doubt, please check with your manager/leader. All organisations and individuals should normally have signed confidentiality and data processing agreements, or sign employment contracts with confidentiality and data processing clauses before they are given access to, or otherwise process personal data. Where this is not possible, please contact the DPO for consideration.

Processing information accurately

Where information is given over the telephone or face-to-face, the information should be read back to the individual or shown to them so that they can confirm it is correct. If an address or similar has been provided incorrectly by an individual, we will contact the individual to confirm the proposed correction before processing.

Transferring data securely

Email has considerable risks.

- Firstly, emails can travel through many servers, in many countries on their journey to the person they are being sent to. Each link and server can be targeted by hackers.
- Secondly, emails can be sent to the wrong person with just a letter missed from an email address or auto-fill populating the wrong person.
- Thirdly, email chains can be forwarded accidentally without realising the data that exists lower in the chain.

The following are permitted.

a) If personal data is emailed from and to Cross Connecting email accounts using Office365 with the Outlook software on a computer or Outlook app on a mobile phone or tablet, then the data and email is automatically encrypted for the sender, receiver and in transit. This is secure.

b) Password-protected spreadsheets are the next best option, but the password must be sent using a different medium of communication, such as SMS or phone call, so that the data and the password cannot be linked together by a third party.

Post

a) Seal in robust packaging to prevent accidental loss or temptation to tamper.

b) Send to a named individual and mark 'private and confidential'.

c) Give the return address or contact number on the back in case the package cannot be delivered.

d) Use Royal Mail 'Special Delivery' or a trusted Courier Service where we have an ongoing contract allowing tracking and signed receipt.

Portable computers, tablets, mobile phones or removable media

a) They should be stored and handled in such a way as to minimise the likelihood of loss or theft – not being left in open view in a car or public place.

b) When not in use or unattended, they should be locked in a secure location.

c) With the exception of removable media, they should support remote-disabling and data-wiping. By pre-registering for this capability, you can send a signal to a lost or stolen device to locate it and, if necessary, securely delete all data.

d) Where possible, these should all be fully-encrypted. This is so that unauthorised people cannot access any personal data should it be accidentally mislaid or stolen.

Monitors and screens

Monitors and screens should not show confidential information to passers-by. The following steps will protect personal data.

- "Lock" your computer or device whenever you leave them unattended. Auto-starting password-protected screen-savers should be set.
- Check your screen angle and location so that personal data is not visible to strangers.
- If you are aware of personal information being viewed, photographed, or stolen by unauthorised people, please report it immediately to the Data Protection Officer.

Saving work and electronic files

All documents, files, photographs, videos and data should be saved as directed by your manager/leader This must be on the secure, shared storage approved by the DPO (Office365 Sharepoint).

Documents and personal information should not be saved on personal drives on the servers, on internal or external hard drives on computers, or on personal cloud storage, tablets, mobile phones, DVDs, CDs or other removal media.

However, there could be times when access to the approved shared storage is, might, or will be limited.

- Great care must be taken when saving to these computers or devices. The computers and devices must be made known to the DPO.
- Any work or data should be transferred back to the approved, secure, shared storage as soon as is possible - and then deleted from the computer or device.

Physical security

a) At any location of physical storage of personal data, doors and windows should be closed and locked when unattended.

b) No uncontrolled access should be possible by others who share or enter the Cross Connecting storage locations.

c) Security codes should be changed when a member of staff or volunteer leaves.

d) The DPO will provide lockable storage for all personal and other confidential papers, removal media, portable drives and other electronic devices. Where necessary this storage will also be fire-proof.

e) The locations and owners of all locks and keys should be documented by the DPO.

Organisational security

a) The Data Protection Officer should control and record who has electronic access to all data on Sharepoint.

b) Each user should have and use their own unique username and password.

c) Access should be standardised to role-based profiles wherever possible, giving the appropriate permissions for the role they are fulfilling.

d) When people leave:

- User accounts, passwords and all physical and electronic access should be cancelled.
- The DPO should recover all documents, photos, videos, personal data and other assets held through working or helping Cross Connecting. These should be retained or deleted as necessary.

e) All software used for Cross Connecting, and all software on Cross Connecting devices, must be properly licensed and approved by the DPO.

f) All system and software alerts, messages, patches and updates must be acted on. If you are uncertain on what to do, ask your manager. If automatic updates are not available on your computer or device, you may have old or unauthorised equipment in error and this should be flagged to the DPO.

g) Recent nationwide cyber-attacks have sent corrupt emails to organisations. When these malware emails are opened, whole networks come under attack, ransoms are demanded, and organisations are brought to their knees. Do not click on or open emails where you are unsure of the sender, links or attachments. Also watch out for "phishing" emails where thieves are trying to trick you into providing passwords, bank details and other personal information by claiming to be an organisation or someone that you know – the style of email and the words used will appear identical. Always check with the DPO before clicking or opening them.

h) Administrator level accounts should only be provided to individuals who have been authorised by the DPO. In addition:
    - they should only be used for agreed administrator tasks and not general usage
    - the DPO will maintain a list of those with administrator-level access and will review the list every six months
    - administrator level passwords should be changed every two months

i) The DPO will maintain an IT equipment register so that the owner and location of all computers, devices and removable media holding personal data, past and present, is documented, whether owned by Cross Connecting or otherwise.
    - Each item will have a named owner who shall be responsible for the information security on the item.
    - The register will allow the tracing of the source, ownership, modification, location and disposal of each item, as well as the data residing on the item.
    - All Cross Connecting data shall be securely wiped from each item before it is disposed of, sold or transferred.

j) Employee and volunteer handbooks and individual contracts and agreements should contain a statement concerning the handling and misuse of personal data.

k) Social media - Cross Connecting maintain a number of social media accounts. Access is controlled by one of the directors and must be protected by strong passwords in line with this policy. Approved users of Cross Connecting accounts are representatives of Cross Connecting and must behave responsibly while using social media.

Technical security

We will meet the standards of the UK Government's Cyber Essentials Scheme, understanding that we will review the current policy of permitting personal devices for Cross Connecting work:

a) Internet gateways – should prevent staff and volunteers accessing websites or other online services that present a threat to Cross Connecting systems or that we do not trust.

b) Purchases, modifications and disposals of hardware and software – must be reviewed and approved by the DPO. Hardware should be recorded on the IT

Equipment register. All purchases and modifications of hardware should be correctly sized, include security requirements, be assessed for the purposes needed, set up with the necessary software and be compatible with existing and planned systems.

c) Secure configuration - Hardware and software must be set-up and configured adequately by the DPO to provide effective protection.

d) Software and services – unused or unauthorised software should be removed from Cross Connecting devices, computers, servers and networks to reduce potential vulnerabilities.

e) Anti-virus and anti-malware software:

- is installed on Cross Connecting computers and devices to prevent or detect threats from malicious software and viruses;
- scans files and data on each device daily and when files are accessed;
- automatically checks for and installs updates daily; and
- blocks access to malicious websites.

f) Patch management and software updates – all Cross Connecting software is patched and updated at all times. Systems, servers, networks, computers and devices will be set to automatically update, and this will be checked to ensure that all updates are installed within 7 days of release

g) Processing by external data processors inside and outside of the UK - we only transfer personal information with suitable safeguards and where it can be adequately protected. Written contracts should be in place with each of these organisations, including external cloud services, so that personal information is transferred, processed and stored confidentially, legally and securely.

h) The Cyber Essentials standard for Data Security requires an annual external audit of vulnerabilities from Cloud providers and also all external IP addresses. It also requires regular updates to Data Security Risk Assessments, as well as any Business Continuity Plans and the Disaster Recovery Plans.

i) Mobile devices -

- All mobile devices used for Cross Connecting must be approved in advance by the DPO and registered on the IT Equipment register, whether owned by Cross Connecting or otherwise.
- Such devices must be PIN/password protected, be encrypted if available, should be capable of being remotely wiped and should have anti-malware software installed if available.
- Wherever possible, Cross Connecting documents and data should be kept in secure databases and not downloaded onto phones.

- Users should inform the DPO if a device is lost or stolen and they will work with the owner to assess the risk to people, wipe Cross Connecting data from the device and change all passwords.

j) Remote working – Microsoft Office365 communications and file usage are secure from your device to another Cross Connecting person wherever you are working. Where you are not working in Microsoft Office365, staff and volunteers should wherever possible limit the sending, downloading or uploading of people's personal data over open, unsecure Wi-Fi networks, low-security home routers or Bluetooth connections. 4G mobile hotspots are significantly more secure than open Wi-Fi networks. Based on ministry need and the level of risk, the DPO may provide a VPN or other solution to secure data while remote working (typically if working overseas).

k) Cross Connecting reserves the right to monitor systems and communications where it suspects that there has been a breach of this policy in accordance with the Regulation of Investigatory Powers Act (2000).

The Rights of Individuals

The right to privacy

This policy explains how we respect the privacy of everyone that we have contact with. The policy is relevant to anyone we are in contact with and collect data from, whether on a paper form or electronically on our website.

Whenever the data protection policy is changed, we will communicate the new policy to those who have given us their contact details and consented to stay in touch. It will also be published on the Cross Connecting website.

The rights to be informed, access, amend, transfer and delete information

Individuals can contact Cross Connecting to:

- be informed as to the purpose of the data processing and the lawful basis for this processing;
- access their personal data and to request rectification or deletion if it is inaccurate or incomplete;
- restrict and/or object to the processing of their data;
- transfer their personal data - allowing them to move, copy or transfer the personal data that we hold to another organisation in a safe and secure way; or

- receive a copy of all of their personal data, whether held on computer or paper. This is formally known as a subject access request and needs to say why the information is processed, anyone it may be disclosed to, and the source of the data. The request may merely say, "I want to see what you hold about me".

These requests may require us to take legal advice and so all requests should be directed immediately **to the Data Protection Officer** by email to hello@crossconnecting.co.uk .

The Data Protection Officer will check the identity of the person requesting, acknowledge receiving the request, log the request and respond accurately and completely without delay and at the latest within one month of receipt.

Cross Connecting may extend the response period by a further two months where requests are complex or numerous. If we do, we will inform the individual within one month of the receipt of the request and explain the reason for the extension.

If a request remains unresolved, individuals can complain to the Information Commissioner's Office at https://ico.org.uk/concerns.

Data Retention

Cross Connecting hold personal information for *only* as long as is necessary.

At least once each year, information beyond the timescales below should be deleted safely and securely, by each department.

The timescales are:

- Current year + 6 years: financial (excluding contracts, estimates, quotations, cash book, nominal ledger and asset registers), stores records, records (excluding annual earnings summaries), subcontractor records, taxation records, project files and ordering records (excluding contracts).
- Leaving date + 6 years: staff who have not been in contact with young people - personnel, redundancy and training records.
- Current year + 7 years: customer complaints.
- End of benefits + 10 years: pension details.
- Current + 12 years: annual earnings summaries, asset registers, cash book, sales ledger, purchase ledger, journal entries.
- Expiry + 12 years: group health and staff personal policies, contracts, quotations, estimates, title deeds, planning permissions and property documents.

Not deleted at the moment: employment decision documents, where staff have been in contact with young people – their personnel, redundancy and training records, all accident records, health and safety assessments and consultations; safeguarding reports; DBS staff and volunteer checks, quality control records, medical records, insurance policies.

Never deleted: public and product liability policies, trade mark papers, nominal ledger, Director records, meeting minutes, and statutory accounts.

Disposing of Old Data Securely

All deleting of personal information should comply with this policy and be approved by your manager because of the possible legal implications.

a) Paper documents should be shredded.

b) Files on computers, laptops, tablets, mobile phones and removal media should be deleted, along with all back-up copies.

c) Unfortunately, most devices and removable media retain personal data even after deleting. So, the DPO will check if the devices are fully encrypted and if not, they will manage the certified shredding and where appropriate the replacement of memory chips when equipment or devices are transferred, sold, or reach end-of-life, or when staff or volunteers leave. This will prevent deleted personal data being recovered by identity thieves.

d) Where staff or volunteers use or have used their own personal devices or removable media and they are to be sold, transferred or disposed of, the DPO will check if they are fully-encrypted and if not, will pay for and if agreeable, organise the certified shredding and, where appropriate, replace the memory chips.

e) Where staff or volunteers leave Cross Connecting and they use or have used their own personal devices or removable media for Cross Connecting, at some stage the staff or volunteers will dispose of, transfer or sell that equipment. Unless they are fully encrypted, Cross Connecting personal data remains accessible on the memory chips. The ex-staff or volunteer will notify the DPO, who will then pay for and if agreeable, organise the certified shredding and, where appropriate, replace the memory chips.

Cookies

What are cookies?

Cookies help organisations improve how websites display on devices and improve how they function for people. They are small, anonymous, unique strings of text sent from websites to people's devices (the internet browser and the hard drive) when people visit websites.

Our use of cookies

Our websites send two cookies.

- One cookie allows us to know when someone's device returns to the website. If they log into our websites, this session cookie is key to staying logged in during the visit. If we have to investigate a problem, the cookie allows us to retrieve the last date, time and web-page that they visited the website. Session details are only stored temporarily (normally less than 24 hours) and the cookie effectively expires as soon as the internet session expires.

- The other cookie helps us to see how the website is performing and used. This Google Analytics cookie allows us to collect the "IP address" allocated to people's devices that day (not your name), the type of browser and device, any anonymous socio-demographic information that Google has consent from them to share, any links that they have used to get to the website, the pages they have visited and for how long. Google Analytics aggregates the information for all users so that we can identify where the website isn't working well, how people arrive at the website, and how we can improve our services and the use of our services. We do not combine the information with other personal data to identify people. You can read Google's policy here: https://policies.google.com/privacy.

Third party cookies and pixels

We use YouTube to embed videos on our websites and they may send cookies to people's devices. We cannot control cookies from these or any other third-party websites, but the privacy statements explain how they are used.

We use social media providers such as Facebook and Instagram to let people know about our events. They use cookies and "pixels" to track the effectiveness of adverts.

Managing cookies and pixels

Our websites will only function properly when the two cookies are fully operating, but people can block or limit how cookies work on their devices under “Settings” in their internet browser and can also block the Google Analytics cookie at https://tools.google.com/dlpage/gaoptout.

Social media cookies and pixels can be managed by changing the settings on social media accounts, internet browsers and email accounts. People can also opt-out of or limit how advertising cookies and pixels work on devices with the Network Advertising Initiative. See http://optout.networkadvertising.org/ and the Digital Advertising Alliance website http://optout.aboutads.info/.

Independent Supervisory Authority

The Information Commissioners Office (ICO) is the independent supervisory authority set up to promote and oversee compliance with Data Protection Legislation in the UK. You can contact the Information Commissioner's Office via their website at www.ico.org.uk.