



General Data Protection Regulation (GDPR) Policy

Revised April 2024

Contents:

Ref	Title	Page
	Introduction	2
1	Purpose	2
2	Policy	3
3	Key risks	3
4	Roles and responsibilities	3
5	Retention	3
6	Access and security	4
7	Data breach	4
8	Third Party Processor Agreements	5
9	Data Protection Impact Assessment (DPIA) Procedures	5
10	Identified use of personal information	5
10.1	The Company Membership	6
10.2	Event Sales and Marketing	7
10.3	Applicants and residents of the Company's Almshouse schemes	8
10.4	Grant applicants and beneficiaries of the Company's grant making schemes	10
10.5	School and trustees of the Skinners' Academies Trust Board and links to the Company's schools.	11
10.6	Skinners' Company Fundraising and Supporters.	13
10.7	Skinners' Company staff and GDPR working practices	15
	Personal Data Breach Action Plan	17

Introduction.

The Skinners' Company takes its responsibility towards its stakeholders' personal privacy seriously.

Stakeholders are defined as:

- The Company Membership and Membership applicants.
- Applicants and residents of the Company's Almshouse schemes.
- Grant applicants and beneficiaries of the Company's grant making charities.
- School Governorship and links to the Company's schools.
- Donors and legators to the Company and its charities.
- Current and former members of Skinners' Company staff.
- Venue hire clients of Pellipar Services Company Limited (PSC) in tandem with the related policies of the Company's caterer The Blue Strawberry Group (BSG)*.

*Venue hire client details are first received by BSG. Those that book an event are shared with PSC.

The General Data Protection Regulation (GDPR) (2018) regulates the way in which personal data relating to the aforementioned is stored and for what purpose it is kept. Data comprises identifiable information held both electronically and as hard copy.

1. Purpose.

The purpose of this policy is to enable the Company to:

- demonstrate an open and honest approach to the handling of personal data.
- comply with the law in respect of the data it holds about individuals.
- follow good practice.
- protect all personal data.
- protect the Company from the consequences of a breach of its responsibilities.

The purpose of the GDPR is to protect the rights and privacy of individuals and to ensure that data about them is not processed without their knowledge and is processed with their consent wherever possible. The previous Data Protection Act (1998) set out eight principles, which remain now that GDPR has been introduced.

These eight principles are that data must:

1. be processed fairly and lawfully.
2. be obtained only for specified and lawful purposes.
3. be adequate, relevant and not excessive.
4. be accurate and up to date.
5. not be kept for longer than is necessary.
6. be processed in line with individuals' rights.
7. be securely kept.
8. not be transferred to other countries without adequate protection.

The Company's stakeholders/data subjects have the following rights under GDPR:

1. Right to be informed: Individuals have the right to know how their data is being used.
2. Right of access: Individuals can request access to their personal data.
3. Right to rectification: Incorrect or incomplete data can be corrected.
4. Right to erasure: Individuals can request the deletion of their data under certain conditions.
5. Right to restrict processing: Processing of personal data can be limited.

6. Right to data portability: Individuals can request the transfer of their data to another entity.
7. Right to object: Individuals can object to the processing of their personal data.

2. Policy.

Under GDPR, personal data means 'any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Personal data should only be kept where there is a legitimate interest to do so. Once obtained it should be used for a specific and lawful purpose without being processed any further. Any personal data should be limited to only that which is relevant. GDPR states that the data should be kept for no longer than is necessary for the purposes for which the personal data is processed.

The Skinners' Company will ensure that all personal data is fairly and lawfully obtained and processed and securely held, in accordance with these principles. It will:

- comply with both the law and good practice.
- respect individuals' rights.
- be open and honest with individuals whose data is held.
- provide training and support for staff who handle personal data, so that they can act confidently and consistently.

3. Key Risks.

The Skinners' Company has identified the following potential key risks: breach of confidentiality (information being given out inappropriately).

- misuse of personal information.
- individuals being insufficiently informed about the use of their data.
- breach of security by allowing unauthorised access.
- harm to individuals if personal data is not up to date.

4. Roles and Responsibilities.

The Skinners' Company recognises its overall responsibility for ensuring that each entity complies with its legal obligations.

The Clerk/ Chief Executive Officer acts as the Data Protection Officer. The Clerk will:

- ensure Data Protection and related policies remains under constant review.
- ensure Data Protection training takes place for all administrative staff.
- identify and log the personal data kept and ensure its security.
- ensure that only data which is necessary for the Company to fulfil its role is processed.
- keep under review the data which is processed to ensure it remains necessary.
- undertake a Legitimate Interests Assessment and keep this under review.
- inform stakeholders of personal data that the Company holds, the reason that the data is held, for how long the data will be held, how to make a subject access request, their right to rectification and their right to erasure;

- deal with access requests. Requests by an individual for access to their data should be made in writing to the Clerk. Depending on the specific requirements of any request, and on resource availability, the Clerk will endeavour to meet any request within 10 working days.
- ensure staff know how to report a data breach.
- destroy personal data when it no longer needs to be processed.

(The Clerk's/CEO contact details are shown under [section 7: Data Breach](#))

5. Retention.

The Skinners' Company will only process information necessary to carry out its work and to provide or administer activities for Company members, Venue hire events and catering, Almshouse schemes, charitable foundations, School Governance and administration of staff.

Retention of data is determined by the following lead processors:

- Membership, Events and Communications Manager.
- Hall Director- Sales and Marketing.
- Director of the Skinners' Almshouse Charity
- Foundations Manager - Grant giving charities
- Director of Education- School Governorship
- Finance Director- Staff records

The Hall Director ensures the Company has the means to destroy data by shredding hard copy (aided by an off-site shredding company) and deleting electronic files as soon as they are no longer relevant. The Skinners' Company will only keep the information while an individual is a member, Almshouse resident, grant beneficiary or school governor, or as long as necessary for administration purposes up to a maximum of 2-3 years. Past employee details are kept for as long as pension liabilities exist.

6. Access and security.

Access to data stored by the Company is restricted to those with a need to know or those data subjects who formally request access to their personal file.

The following security measures will be used to protect data:

- All hard copies of data are protected in locked storage cabinets in locked offices with restricted access controlled by the Hall Director.
- All electronically stored data is held on a password protected network and on password protected mobile phones. Backups occur daily. Employees set strong passwords and change them regularly.

If a breach of data security is suspected or occurs the Clerk should be informed.

7. Data breach.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. In the event of a data breach, The Skinners'

Company follows a structured Incident Response Plan. This plan outlines procedures for breach detection, containment, assessment, notification, and remediation. It ensures prompt action to minimise harm and comply with legal obligations. Any known breach will be reported by the Skinners' Company to the Information Commissioner's Office (ICO) within 72 hours of its discovery. In the event of a data breach, the Clerk must be informed and the individual(s) whose data is involved in the breach will also be notified. The ICO can apply a fine.

If you suspect a data breach, please contact the Clerk:

by email: clerk@skinners.org.uk

by telephone: 020 7236 5629

by post: The Clerk-The Data Controller
The Skinners' Company
Skinners' Hall
8 Dowgate Hill
LONDON
EC4R 2SP

8. Third-Party Processor Agreements.

When engaging third-party processors, The Skinners' Company ensures that such relationships are governed by contracts that mandate adherence to GDPR and this Data Protection Policy. These agreements require third parties to implement appropriate technical and organisational measures to protect personal data.

9. Data Protection Impact Assessment (DPIA) Procedures.

To ensure the protection of personal data and compliance with GDPR, The Skinners' Company will conduct Data Protection Impact Assessments for any new projects or technologies that involve the processing of personal data. DPIAs will identify and mitigate risks related to data processing activities. The assessment will be carried out at the project planning stage, with results documented and necessary actions taken to address any identified risks.

10. Identified use of personal information.

10.1: The Company Membership.

Use of Members personal Information

The personal information will only be used for the purposes outlined below.

- Administration of membership(s).
- Fulfilment of orders for goods and services requested including ticketing.
- In-house research and statistical analysis.

- Charitable fundraising
- Communication about campaigns, membership, events and other activities.

Processing personal data for the above purpose's entails sharing your information with the Company's trading subsidiary Pellipar Services Company Limited, employees and main contractors including the catering partner when required. Agreements exist between The Skinners Company and such parties that seek to ensure there must be no further disclosure of such personal data.

Members of the Court and Livery: Diary.

It is customary for members of the Court and Livery to have their names and home addresses published in the Company diary.

The diary is posted to members of the Company -including those members who reside overseas.

Members may opt out of this practice by contacting the Clerk- clerk@skinners.org.uk

The City of London Chamberlain's Court.

It is necessary upon taking up Freedom of the City of London via the Skinners' Company, for the Company to provide the City of London's Chamberlain's Court with the recipient's name address and their long format birth certificate, which may also contain identifiable parental information. This information is stored in the Common Hall Register.

The City of London state:

In order to meet our obligations in relation to the register of electors for Common Hall each year, we will share your personal data (name, address, title and livery membership) with the Town Clerk & Chief Executive of the City of London Corporation for electoral purposes pursuant to the City of London Ballot Act 1887. A separate privacy notice setting out how your personal data will be processed by the City of London Corporation is available via:

<https://www.cityoflondon.gov.uk/footer/privacy-notice>

If you have any concerns or questions about how The City of London look after your personal information, please contact the City of London's Data Protection Officer via e-mail:

Information.Officer@cityoflondon.gov.uk

Verifying, updating and amending your Skinners' Company Membership Profile

Your Membership Profile contains:

- Your contact details
- the details of your submitted CV
- Notes / email correspondence generated by staff for internal staff use only about your interests in Company activities including the Company's programme of events, philanthropy, committees and campaigns.

You can edit and update your details in real time.

Access your Membership Profile at any time via the [Members Area](#) of the Skinners' Company website: www.skinners.org.uk

Then click onto the [Edit My Profile](#) button.

If you experience any difficulties logging in to the Members Area of the website or updating your profile please contact the membership team.

By e-mail: membership@skinners.org.uk

By telephone: 0207 2130551

Please note that the Skinners' Company will not be responsible for any errors you might make.

10.2 Event Sales and Marketing.

Commercial hire is overseen by the Company's catering Partner – The Blue Strawberry Group. Information is shared by the Terms of Conditions of Hire and Contract whereby the relevant GDPR policies are outlined.

Provision is made for the legitimate sharing of information such as a the clients Company name and contact name or in the event of private hire, (wedding events etc) The Skinners' Company/ Pellipar Services Company Limited is party to the booking reference name(s) and the contact details of the person paying the bill.

Within the Caterers Terms and Conditions, Clients have the option to decline the sharing of this information- leading to the shared information becoming anonymised.

The shared information is used by The Skinners' Company/ Pellipar Services Company Limited to cross check event activities verses revenue, to monitor overall turnover and used for the internal analysis of venue hire activities.

Client information is not shared beyond the two named parties.

Subject access request

Clients of the venue have the right to make a Subject Access Request direct to the Skinners' Company to ask to view the personal data which we hold.

Verifying, updating and amending your Client information.

In addition to the aforementioned procedures if, at any time, you want to verify, update or amend your personal data or preferences please contact us.

Please provide your full name and date of your Event to help us track your record.

You can contact us as follows:

by email: paul.richards@skinners.org.uk

by telephone: 020 7213 0554

by post:

Hall Director
The Skinners' Company
Skinners' Hall-Eight and a Half London
8 Dowgate Hill
LONDON
EC4R 2SP

Please allow up for 10 working days for us to amend your details.

10.3 Applicants and residents of The Skinners' Company's Almshouse Charity (SAC) Schemes.

Use of Almshouse applicant and resident personal Information.

Applicants applying for accommodation will disclose personal data on their application form. The revised 2018 application form will contain the following clause:

It is part of the trustees' responsibilities to ensure that applicants for Almshouses are eligible under the terms of the charity's governing document. Trustees therefore need to investigate the personal circumstances of applicants. In practice this is done by SAC staff; they are employees of The Skinners' Company. If your application for accommodation is successful, the personal data supplied on this form and other information relating to an Almshouse licensee will be held on file for the duration of your appointment as a resident and for up to three further years. Some details may be checked with relevant organisations, but none will be disclosed for any inappropriate purpose. You may have access to your personal information on request. If your application is unsuccessful, your application form and all other personal data supplied will be deleted and destroyed.

The Skinners' Company Almshouse Charity (SAC) trustees have carried out a Legitimate Interests Assessment which shows that we feel that it is in the interests of both residents and the charity to hold the following data about residents, and if the charity did not hold this data, it would not be able to fulfil its function with regard to support of residents:

- a. Full name and address, phone numbers and email address
- b. Date of birth
- c. Gender
- d. Marital status
- e. NI number
- f. Name and address of GP

- g. Name, address and contact details of 1st next of kin and 2nd next of kin
- h. Details of any Lasting or Enduring Power of Attorney that is in place
- i. Name and address of location where their Will is kept (if the resident has one)
- j. Details of their funeral planning arrangements and pre-paid plan (if the resident has one)
- k. Details of bank account (for processing direct debits for WMC collection)
- l. Details of income and savings at the time of application for accommodation
- m. Details of current medical conditions and past operations / hospital admissions / previous conditions
- n. Details of allergies to medicine, e.g. antibiotics

Subject access request.

Residents have the right to make a Subject Access Request direct to the Skinners' Almshouse Charity Director, to ask to view the personal data which we hold. Residents have the right to rectification, i.e. to have incorrect information amended.

At least annually Scheme Managers review the information on your Resident Record Sheet with you, you are asked to amend any data and to sign to say that the data is accurate. Residents should inform SAC of any changes to their personal data prior to this should they arise.

Right to erasure of personal data

Residents also have the right to erasure, i.e. the right to be 'forgotten', if you object to the processing of personal data for legitimate interests. However, you need to be aware that if you exercised the right to erasure, the charity would not be able to fulfil its role in supporting you and ensuring you receive the care you need, for example liaising with your family/friends/next of kin, liaising with your GP/consultants/social services/carers about your health and well-being and enabling the charity's staff to signpost residents to appropriate external care. If a resident requested that their personal data was erased, the charity would make a compelling case for why it needs to process that data.

Retention of Personal information

Residents' personal data is held for a maximum of 3 years after a resident dies or leaves their Almshouse. This is so that the charity can liaise where necessary with a resident's next of kin and/or with a nursing home or care home. All personal data is then destroyed.

Verifying, updating and amending your Almshouse Charity personal information.

In addition to the aforementioned-procedures if, at any time, you want to verify, update or amend your personal data or preferences please contact us.

Please provide your full name and date of birth, to help us track your application/resident record. You can contact us as follows:

by email: caroline.hamilton@skinners.org.uk

by telephone: 020 7213 0576

by post:

Director of the Skinners' Almshouse Charity
The Skinners' Company
Skinners' Hall
8 Dowgate Hill
LONDON
EC4R 2SP

Please allow up for 10 working days for us to amend your details.

10.4: Grant applicants and beneficiaries of the Skinners' Company Foundations

- Skinners' Education Foundation
- Skinners' Charity Foundation
- Skinners' Heritage Foundation
- Skinners' Almshouse Foundation
- The Sir Andrew Judd Foundation
- The administration of The Thomas Wall Trust.

Applicants applying for grants are required to disclose personal data on their application form. The application forms contain the following clause:

It is the trustees' responsibility to ensure that applicants for grants are eligible according to the (named) charity's funding criteria. Trustees therefore need to understand the personal circumstances of applicants. Some details may be checked with relevant organisations, but none will be shared for any purpose not linked to grant assessment or administration. You may have access to your personal information on request.

Verifying, updating and amending your grant application personal information.

In addition, if, at any time, you want to verify, update or amend your personal data or preferences please contact us.

Please provide your full name and date of birth, to help us track your application record. You can contact us as follows:

By email: charities@skinners.org.uk

By telephone: 020 7213 0561

By post: The Foundations Manager
 The Skinners' Company
 Skinners' Hall
 8 Dowgate Hill
 LONDON
 EC4R 2SP

Please allow up for 10 working days for us to amend your details.

10.5: School and trustees of the Skinners' Academies Trust Board and links to the Company's schools.

This policy applies to pupils, staff, governors and Trustees of the following schools, who are not members of the Company:

- The Judd School
- The Marsh Academy
- Skinners' Academy
- The Skinners' School
- The Skinners' Kent Academy
- Skinners' Kent Primary School
- Tonbridge School
- The New Beacon School
- Temple Grove Academy
- Skinners' Academies Trust

Use of non-member school governors' personal information.

Personal information will be used for the purposes outlined below.

- Administration of related business.
- Recording of training taken/required.
- In-house research and statistical analysis.

Processing personal data for the above purposes' entails sharing personal information with fellow governors, or Trustees, the governed school or Trust, Companies House, the Charities Commission the Department for Education and its agencies, and related local authorities.

Information is held for the duration of the governor's or Trustee's term of office and for four years or beyond in case the DfE, Ofsted or Companies House required evidence.

Use of pupil and staff personal information.

Under normal circumstances schools and academies do not share the personal data of its pupil or staff population.

However, individual's data may be required by the Skinners' Company in the following instances. In each case their details are handled in accordance with the procedures for all other members of The Company:

- to work in support of exclusions, complaints and appeals processes;
- the small number of students each year who are invited to join The Company; .
- members of staff whose data is collected for the purposes of keeping a Register of Business Interests for schools in the Skinners' Academies Trust;
- members of staff involved in Company events.

Personal data may be collected by Skinners' Academies Trust on pupils and members of staff, for the use of the Trust and not the Company. In such cases the data may be stored on the Company's systems. A Data Sharing agreement exists between the Company and Skinners' Academies Trust to regulate this storage of data.

A Data Sharing Agreement.

A Data Sharing Agreement exists between each of our schools/ academies and the Company in order to regulate this flow of personal data and this forms part of the Privacy Agreement between the schools and the parents.

In these cases, the Skinners' Company will obtain permission via the School to access specific information.

No personal data is held by the Skinners' Company beyond the scope of any inquiry/ process. *(This may mean once an inquiry is finished or beyond for required legitimate- legal purposes).*

Verifying, updating and amending your personal information

In addition to the aforementioned procedures if, at any time, you want to verify, update or amend your personal data or preferences please contact us.

Please provide your full name and date of birth to help us track your record. You can contact us as follows:

By email: skinners.ed@skinners.org.uk

By telephone: 020 7213 0556

By post:

Director of Education
The Skinners' Company
Skinners' Hall
8 Dowgate Hill

LONDON
EC4R 2SP

Please allow up for 10 working days for us to amend your details.

10.6 Skinners' Company Fundraising and Supporters.

The Skinners' Company Development team develops and manages relationships with our supporters. We aim to raise funds to support the Company charities. We work closely with staff, members, and our current supporters to support our schools, heritage, Almshouses and Grant-making objectives.

What data do we process?

We will process your personal data only for specified purposes to provide you with a more efficient and personalised service. We seek to ensure that all personal data captured is adequate and relevant to that purpose.

We collect the following data:

- name, address, phone number or email address
- information regarding your relationship with The Company, including events you have attended, donations you have made and communications you have had with members of staff;
- details of any donation you may have made to The Company charities including how it was received (e.g. cheque, direct debit, CAF, online), date of receipt and whether Gift Aid is applicable. We then use stored contact details to properly thank and steward any donation you make;
- information regarding your personal preferences, philanthropic history, and capacity to donate. This may include information provided through publicly available sources such as LinkedIn and news feeds.

Our members act as ambassadors for our work and these ambassadors will provide us with information on those, they consider having a legitimate interest in our charitable work. We will never contact an individual unless they have given us or our ambassador's permission to do so.

What do we use your data for?

We use your data to:

- fulfil our obligations to supporters in terms of acknowledging gifts and agreed stewardship activities;
- administer donations or other payments (such as event tickets);
- keep you updated on Company activities that are relevant to you;
- offer you opportunities to engage further with our activities;
- fundraise further on behalf of The Company
- administrate Gift Aid claims;
- prepare for events that you attend. The Development team may compile event briefing notes for our team. This will include information such as your relationship with The Company and your philanthropic interests. These briefing notes will not be shared beyond members of staff and our senior volunteers.

How do we store your data?

Your data will be kept confidential. Personal data is always stored on password protected computers only available to members of staff with a login. Personal data on hard copy is stored in locked cupboards. We also store bank and other payment details in secure systems as appropriate.

How are payment processing and security measures handled?

Payment Processing and Security Measures: The Skinners' Company uses Stripe and GoCardless as our payment service providers to securely process donations and other financial transactions, such as event ticket purchases. All payment information is transmitted securely and managed according to the privacy policies and security measures of these providers, both of whom comply with the highest industry standards (PCI DSS compliant). This ensures robust protection of your financial data, which is not stored on our systems but handled exclusively through encrypted channels by Stripe and GoCardless. This approach not only safeguards your financial information against unauthorised access but also ensures compliance with GDPR.

What is the lawful basis for processing your data?

Current and former supporters

We rely on legitimate interest when processing information relating to current supporters and recent former supporters.

New or prospective supporters

For new or prospective supporters, we will rely on an individual's consent.

How long do we retain your data?

The personal data we collect are evaluated annually to determine whether they are current and still need to be held. There may be legal requirements that require us to retain your data e.g. tax regulations and the Charities Act 2011.

How do you opt out?

You may opt-out from receiving correspondence from the Development team at any time by emailing donate@skinners.org.uk

10.7: Skinners' Company staff–

Including staff GDPR working practices

The Skinners' Company holds the following personal data on staff:

1. Full name and address, phone numbers and email address
2. Date of birth
3. Gender
4. NI number
5. Name, address and contact details of next of kin
6. Details of bank accounts (for processing payment)

The Clerk/ Chief Executive has carried out a Legitimate Interests Assessment which shows that the Skinners' Company believes it has a legitimate interest to hold the above personal data for staff and that we would not be able to perform our job in supporting staff without this information.

The Skinners Company must ensure that it only holds data for staff that is absolutely necessary; the Company must not hold inaccurate data, nor hold data for longer than is necessary; the Company must have a procedure for destroying data and must ensure that staff data (both hard copy and electronic) is protected.

It's possible that The Company will hold information about employee's health and disabilities when they are provided in the context of requests for reasonable adjustments.

Past employee details are kept for as long as pension liabilities exist.

Staff GDPR working practices

All computers and laptops must be password protected. The passwords must be STRONG (comprising letters - some uppercase some lowercase, numbers and ideally other characters as well). All staff must change their computer or laptop sign on password on receipt of this protocol and change it regularly.

1. Laptops and computers must be either switched off or logged off when not in use.
2. Staff must ensure that, when their computer goes into 'sleep' mode, the password has to be re-entered to wake the computer up again.
3. Block send e-mails- e-mail addresses should be entered into the Bcc address box to ensure e-mail addresses are not shared. Alternatively block send e-mails can be posted via the CRM system to ensure e-mail addresses are not shared.
4. Staff must ensure that, no unauthorised persons have sight of personal data displayed on screens
5. Mobile phones onto which are downloaded Personal data must be password protected and passwords must be STRONG. *It is recommended to use a combination of three random words with numeric.*
6. Staff must ensure that paper files which contain personal data are kept in a locked filing cabinet.
7. Old diaries should be kept in a locked cabinet or shredded.
8. Staff must ensure that no hard copies of personal data on is left out on desks overnight.
9. No personal data must be put on noticeboards in the offices.
10. All staff must regularly go through their computer files and delete all documents with personal data which are no longer needed or out of date.

Other important things for Company staff (data processors) to note in relation to The Skinners' Company's GDPR policy:

1. The Right to Erasure

All data subjects have the right to erasure, i.e. the right to 'be forgotten' and legally The Skinners' Company has to make them aware of this. Documentation should make it clear to all data subjects that if they were to exercise this right, the Company would not be able to do their job properly.

2. Subject Access Requests

All Company related data subjects have the right to make a Subject Access Request - i.e. to ask to see all their personal data/correspondence with them or about them that the Company holds and to have copies of everything. If a Data Subject asked for this, the Company would be legally obliged to show them everything. Therefore, it is vital that staff have nothing written down that staff would not wish the data subject to read.

3. Data disposal

When disposing of hard copies of personal data, it must be shredded.

4. Data breach

Staff are required to be vigilant about possible data breaches which could occur through hacking/phishing. If in doubt about the source of an email or whether it is genuine, please do not open it and check with the Hall Director or IT support first. (Virtual IT: 0207 6442820)

If staff suspect a data breach (e.g. that personal data has got into the public domain) please report it to the Clerk asap., who will report it to the Information Commissioner's Office within 72 hours.

Staff must ensure that they always enable Windows updates when prompted.

Personal Data Breach Action Plan

The Clerk is the Data Comptroller.

The Clerk is to be notified of any suspected data breach.

The following actions are required:

- **Ascertain Details of the breach** – a general overview of the breach, the date and time it happened and when it was discovered.
- **Details of staff members** – was a specific member of staff involved and what data protection training they've had.
- **Details of the data and people affected** – how much data and how many people have been affected and the possible risk to individuals as a result of the breach.
- **What efforts have been employed to contain the breach** - what preventative measures were in place beforehand, what actions you've taken to stop it happening again and what other organisations you have told or need to tell about the breach.

The Information Commissioners Office ICO must be notified within 72 hours of the discovery of a breach [Report a data breach online form | ICO](#)

On line personal data is stored and backed up via the Company's Microsoft 365 Network Drives.

Skinners Company MS network managed by Virtual IT: 0207 6442820

Salesforce CRM Account Executive Cian Elliott cian.elliott@salesforce.com

